



Sybase Control Center for SAP Sybase IQ

3.2.7

DOCUMENT ID: DC01267-01-0327-02

LAST REVISED: April 2013

Copyright © 2013 by SAP AG or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.

Contents

About Sybase Control Center for SAP Sybase IQ	1
New Features in Sybase Control Center for SAP	
Sybase IQ	1
User Interface Overview	4
Toolbar Icons	5
Status Icons	6
Common Display Options	7
Keyboard Shortcuts	10
Displaying the Versions of SCC Components	11
Style and Syntax Conventions	12
Accessibility Features	14
Sybase Control Center Accessibility Information	15
Get Started	17
Quick Start for an Evaluation	17
Get Started in a Production Environment	28
Deploying an Instance from a Shared Disk Installation	
.....	72
Enabling and Disabling Shared-Disk Mode	74
Shared-Disk Mode	74
sccinstance Command	75
Launching Sybase Control Center	80
Registering the ODBC Driver in Windows	80
Starting and Stopping Sybase Control Center in	
Windows	81
Starting and Stopping Sybase Control Center in	
UNIX	84
Configuring Memory Usage	88
scc Command	91
Logging in to Sybase Control Center	95
Logging out of Sybase Control Center	96
Setting Up Security	96

Security	97
Configuring Authentication for Windows	98
Configuring a Pluggable Authentication Module (PAM) for UNIX	99
Configuring an LDAP Authentication Module	101
Mapping Sybase Control Center Roles to LDAP or OS Groups	111
Encrypting a Password	113
Configuring Ports	114
Configuring the E-mail Server	116
Configuring the Automatic Logout Timer	117
Configuring Retrieval Thresholds for the Administration Console	118
User Authorization	119
Assigning a Role to a Login or a Group	119
Removing a Role from a Login or a Group	120
Adding a Group	121
Removing a Group	121
Adding a Login Account to a Group	122
Removing a Login Account from a Group	122
Adding a Login Account to the System	123
Removing a Login Account from the System	124
Modifying a User Profile	125
Logins, Roles, and Groups	125
Configure Sybase Control Center	127
Configuring SAP Sybase IQ Authority-Based Users for Monitoring	128
Configuring SAP Sybase IQ Roles-Based Users for Monitoring	129
Registering an SAP Sybase IQ Server	130
Configuring SAP Sybase IQ for Administration	132
Simplex Privilege Summary	133
Multiplex Privilege Summary	134
Logical Server Privilege Summary	139
Logical Server Policy Privilege Summary	141

Remote Server Privilege Summary	142
External Login Privilege Summary	143
Database Privilege Summary	144
Table Privilege Summary	147
Table Column Privilege Summary	159
Table Permissions Privilege Summary	162
Table Constraints Privilege Summary	163
Table Index Privilege Summary	169
Table Trigger Privilege Summary	174
Table Partition Privilege Summary	176
View Privilege Summary	184
View Permissions Privilege Summary	188
View Trigger Privilege Summary	189
Materialized View Privilege Summary	191
Materialized View Permissions Privilege Summary	198
Materialized View Index Privilege Summary	199
Domain Privilege Summary	202
Text Configuration Privilege Summary	203
Text Index Privilege Summary	206
Sequence Generator Privilege Summary	213
Spatial Support Privilege Summary	216
Authority-Based User Privilege Summary	220
Authority-Based Group Privilege Summary	223
Authority-Based Database Object Permissions Privilege Summary	226
Role-Based User Privilege Summary	228
Role-Based User-Extended Role Privilege Summary	232
Role-Based Standalone Role Privilege Summary	237
Role-Based Database Object Permissions Privilege Summary	242
Role-Based System Role Privilege Summary ...	245

Role-Based Compatibility Role Privilege Summary	247
Role-Based System Privilege Privilege Summary	248
Login Mapping Privilege Summary	249
Login Policy Privilege Summary	251
LDAP Server Configuration Object Privilege Summary	252
DbSPACE Privilege Summary	254
DB File Privilege Summary	256
Event Privilege Summary	258
Java External Environment Privilege Summary	261
Perl External Environment Privilege Summary	262
PHP External Environment Privilege Summary	264
Other External Environment Privilege Summary	266
Function Privilege Summary	266
Procedure Privilege Summary	271
Web Service Privilege Summary	276
Importing Resources for Batch Registration	277
Registering and Authenticating a Sybase Control Center Agent	279
Viewing Sybase Control Center Agent Connection Information	280
Creating a Perspective	281
Adding a Resource to a Perspective	281
Authenticating a Login Account for a Managed Resource	282
Match Case in sysuser for Authentication User ID	282
Changing Update Frequency for Statistics and Charts	282
Setting Up Statistics Collection	283
About Statistics	285
SAP Sybase IQ Data Collections	286

Creating an Alert	295
SAP Sybase IQ Alerts	298
Alert Types and Severities for SAP Sybase IQ	302
Alert-Triggered Scripts	303
Alert-Triggered Script Examples	304
Substitution Parameters for Scripts	305
Key Performance Indicators for SAP Sybase IQ	307
Optional Configuration Steps	317
Administer and Monitor SAP Sybase IQ	319
Displaying Resource Availability: the Heat Chart	319
Graphing Performance Counters: the Statistics Chart	320
Administration Console	321
Browsing and Managing Resources	321
Searching and Filtering Resources	322
Features Not Supported by a Database Version	324
Executing a SQL Query	324
Simplex Servers	325
Monitor Simplex Servers	325
Administer Simplex Servers	347
Multiplex Servers	365
Monitor Multiplex Servers	365
Administer Multiplex Servers	379
Logical Servers	416
Monitor Logical Servers	416
Administer Logical Servers	419
Administer Logical Server Policies	429
Remote Servers	437
Creating a Remote Server	437
Testing a Remote Server Connection	439
Deleting a Remote Server	440
Generating Remote Server DDL Commands	441

Viewing or Modifying Remote Server Properties	442
Remote Server Privilege Summary	444
External Logins	445
Creating an External Login	446
Deleting an External Login	447
Generating External Login DDL Commands	448
Viewing External Login Properties	449
External Login Privilege Summary	450
Databases	451
Creating a Database	451
Creating a Database Using a CSV File	455
Setting Database Options	456
Viewing or Modifying Database Properties	457
Database Privilege Summary	463
Tables	466
Creating a Table	466
Creating a Global Temporary Table	474
Creating a Proxy Table	479
Viewing Table Data in the Execute SQL Window	481
Deleting a Table	483
Generating Table DDL Commands	484
Moving a Table to Another Dbspace	486
Validating a System Store Table	488
Setting the Primary Key	489
Setting a Clustered Index	492
Merging Table Data from RLV Store with IQ Main Store	493
Calculating the Number of Rows in a Table	495
Moving Table Objects to Another Dbspace	497
Enabling or Disabling Row-Level Versioning in a Table	499
Viewing or Modifying Base Table Properties	501

Viewing or Modifying Global Temporary Table	
Properties	506
Viewing and Modifying Proxy Table Properties .	512
Table Privilege Summary	515
Table Columns	528
Table Permissions	543
Table Constraints	556
Table Indexes	586
Table Triggers	606
Table Partitions	617
Views	647
About Views	647
Creating a View	648
Viewing View Data in the Execute SQL Window	
.....	650
Recompiling and Enabling a View	651
Disabling a View	652
Deleting a View	653
Generating View DDL Commands	655
Viewing or Modifying View Properties	656
View Privilege Summary	660
View Permissions	663
View Triggers	679
Materialized Views	687
Creating a Materialized View	689
Viewing Materialized View Data in the Execute	
SQL Window	691
Refreshing Materialized View Data	692
Truncating Materialized View Data	695
Validating Materialized View Data	696
Setting a Clustered Index	698
Recompiling and Enabling a Materialized View .	699
Disabling a Materialized View	701
Deleting a Materialized View	702

Generating Materialized View DDL Commands	703
Viewing or Modifying Materialized View	
Properties	705
Materialized View Privilege Summary	712
Materialized View Permissions	719
Materialized View Indexes	733
Domains	746
Creating a Domain	746
Deleting a Domain	751
Generating Domain DDL Commands	752
Viewing Domain Properties	753
Domain Privilege Summary	754
Text Configuration Objects	755
Creating a Text Configuration Object	755
Deleting a Text Configuration Object	758
Generating Text Configuration Object DDL	
Commands	760
Viewing or Modifying Text Configuration Object	
Properties	761
Text Configuration Privilege Summary	764
Text Indexes	766
Creating a Text Index	766
Deleting a Text Index	769
Refreshing a Text Index	770
Truncating a Text Index	773
Generating Text Index DDL Commands	775
Viewing or Modifying Text Index Properties	777
Text Index Privilege Summary	781
Sequence Generators	788
Creating a Sequence Generator	788
Deleting a Sequence Generator	790
Restarting a Sequence at Start Value	792
Generating Sequence Generator DDL	
Command	793

Viewing or Modifying Sequence Generator	
Properties	794
Granting Sequence Generator USAGE	
Permission	797
Revoking Sequence Generator USAGE	
Permission	798
Sequence Generator Privilege Summary	799
Spatial Support	802
Creating a Spatial Reference System	803
Deleting a Spatial Reference System	805
Generating Spatial Reference System DDL	
Commands	806
Viewing or Modifying Spatial Reference System	
Properties	807
Creating a Spatial Unit of Measure	812
Deleting a Spatial Unit of Measure	815
Generating Spatial Unit of Measure DDL	
Commands	816
Viewing or Modifying Spatial Unit of Measure	
Properties	817
Spatial Support Privilege Summary	819
Security and User Management	822
Authority-Based Security	823
Role-Based Security	891
Login Mappings	1109
Login Policies	1116
LDAP Servers	1133
Dbspaces	1148
Creating a Dbpace	1148
Deleting (Dropping) a Dbpace	1150
Preallocating Space for a Dbpace	1151
Generating Dbpace DDL Commands	1152
Changing a Dbpace to Read-Only	1153
Viewing or Modifying Dbpace Properties	1154
Granting Dbpace CREATE Permission	1157

Revoking Dbospace CREATE Permission	1158
Dbospace Privilege Summary	1159
DB Files	1161
Creating a DB File	1162
Deleting a DB File	1164
Emptying a DB File	1165
Generating DB File DDL Commands	1166
Viewing or Modifying DB File Properties	1167
DB File Privilege Summary	1169
Events	1171
Creating an Event	1171
Deleting an Event	1174
Disabling an Event	1175
Enabling an Event	1176
Triggering an Event	1177
Generating Event DDL Commands	1178
Viewing or Modifying Event Properties	1179
Event Schedules	1181
Event Privilege Summary	1186
External Environments	1189
Working in a Java External Environment	1189
Working in a Perl External Environment	1204
Working in a PHP External Environment	1215
Working in a C ESQL External Environment ...	1226
Working in a C ODBC External Environment .	1228
Working in a CLR (.NET) External Environment	
.....	1230
Functions	1232
Creating a Watcom SQL or Transact-SQL	
Function	1233
Creating an External Java Function	1235
Creating an External C/C++ Scalar or Aggregate	
Function	1237
Deleting a Function	1239
Generating Function DDL Commands	1240

Viewing and Modifying a Function	1241
Granting Function EXECUTE Permission	1244
Revoking Function EXECUTE Permission	1245
Function Privilege Summary	1246
Procedures	1251
Creating a Procedure	1252
Creating a Remote Procedure	1254
Creating a Table UDF or TPF	1257
Executing a Procedure, Table UDF, or TPF using View Data in SQL	1259
Deleting a Procedure, Table UDF, or TPF	1260
Generating Procedure, Table UDF, or TPF DDL Commands	1261
Viewing or Modifying a Procedure, Table UDF, or TPF	1263
Granting Procedure EXECUTE Permission	1266
Revoking Procedure EXECUTE Permission ...	1267
Procedure Privilege Summary	1268
Web Services	1273
Creating a Web Service	1274
Enabling a Web Service	1279
Disabling a Web Service	1280
Deleting a Web Service	1281
Generating Web Service DDL Commands	1282
Viewing or Modifying Web Services Properties	1283
Web Service Privilege Summary	1286
Manage Sybase Control Center	1289
Job Scheduling	1289
Executing and Stopping a Data Collection Job	1289
Deleting a Data Collection Job	1290
Resuming and Suspending a Data Collection Job	1290
Adding a New Schedule to a Job	1291

Viewing or Deleting a Schedule	1292
Modifying the Data Collection Interval for a Job	1293
Resuming and Suspending the Scheduler	1293
Viewing the Job Execution History	1294
Alerts	1294
Types, Severities, and States	1295
Viewing Alerts	1296
Modifying an Alert	1297
Testing an Alert-Triggered Script	1297
Deleting an Alert	1298
Alert Subscriptions	1299
Alert Notifications	1301
Resources	1303
Unregistering a Resource	1303
Adding a Resource to a Perspective	1304
Removing a Resource from a Perspective	1304
Modifying a Resource's Name and Connection Properties	1305
Searching for Resources in the Resource Explorer	1306
Perspectives	1306
Creating a Perspective	1307
Removing a Perspective	1307
Renaming a Perspective	1307
Views	1308
Managing a View	1308
Arranging View Layout in a Perspective	1309
Instances	1310
Enabling and Disabling Shared-Disk Mode	1310
Deploying an Instance from a Shared Disk Installation	1311
Refreshing or Converting an Instance	1312
Removing an Instance	1313
Shared-Disk Mode	1314

sccinstance Command	1315
Repository	1320
Scheduling Backups of the Repository	1320
Modifying the Backup Schedule	1321
Forcing an Immediate Backup	1322
Restoring the Repository from Backups	1323
Configuring Repository Purging	1324
Logging	1325
Viewing the Sybase Control Center for Sybase	
IQ Log	1326
Modifying the Sybase IQ Log Configuration	1326
Using the SAP Sybase IQ Server and SCC	
Agent Logs	1327
Viewing Sybase Control Center Server Logs .	1329
Viewing the Sybase Control Center Client Log	1329
Changing the Logging Level	1330
Logging or Message Levels	1331
Changing Logging Configuration	1331
Sybase Control Center Console	1333
Console Commands	1333
Troubleshoot Sybase Control Center for SAP Sybase IQ	
.....	1337
Problems with Basic Sybase Control Center	
Functionality	1337
Cannot Log In	1337
Sybase Control Center Fails to Start	1337
Browser Refresh (F5) Causes Logout	1338
Alerts Are Not Generated	1338
Performance Statistics Do Not Cover Enough	
Time	1338
Resetting the Online Help	1338
Data Collections Fail to Complete	1339
Memory Warnings at Startup	1340
SCC Out of Memory Errors	1340

Login Fails when Authenticating a Chinese or Japanese SAP Sybase IQ Server	1340
Feature Disabled on the Administration Console Task Menu	1341
My Database Definition is Invalid	1341
Sybase Control Center Is Not Controlling My Multiplex Servers	1342
Fatal Error #2035 Prevents Me from Logging In	1342
Multiplex Node Does Not Appear in Monitor	1343
Multiplex Connection Disallowed by Login Policy	1343
SQL Anywhere Error -131 Appears When Changing A User's Password	1344
Unable to Authenticate After Having Your Password Changed by Another User	1344
Unable to Change Another User's Password	1344
Glossary: Sybase Control Center for SAP Sybase IQ ..	1347
Index	1353

About Sybase Control Center for SAP Sybase IQ

Sybase® Control Center for SAP® Sybase® IQ is a Web-based tool for managing and monitoring SAP Sybase IQ single-node and multiplex servers. The two main features are administration and monitoring.

Sybase Control Center monitoring supports SAP Sybase IQ version 15.3 or later. Sybase Control Center administration supports SAP Sybase IQ version 15.3 or later.

The Sybase Control Center architecture allows a small number of Sybase Control Center servers to monitor all SAP Sybase IQ servers in an enterprise using the Sybase Control Center agent. The Sybase Control Center remote command and control agent (SCC agent) is installed with each SAP Sybase IQ server.

Sybase Control Center for SAP Sybase IQ provides availability monitoring, historical monitoring, and real-time monitoring in a scalable Web application that is integrated with management modules for other Sybase products. It offers shared, consolidated management of heterogeneous resources from any location, real-time notification of availability and performance, and intelligent tools for spotting performance and usage trends, all via a thin-client, rich Internet application delivered through your Web browser.

New Features in Sybase Control Center for SAP Sybase IQ

Brief descriptions of new and enhanced features with links to complete information.

Table 1. New and Enhanced Features in Sybase Control Center for SAP Sybase IQ

Feature	Topics
Role-based security administration – Perform user and role management for role-based users, user-extended roles, and standalone roles. Tasks include create, modify and delete, as well as grant and revoke system privileges and object permissions to users and roles.	<i>Role-Based Security</i> on page 891
Domain administration – Create, view and update domains. The Administration Console tree lists domains under schema objects.	<i>Domains</i> on page 746
External environment administration – In previous releases, only the Java external environment was supported. In SCC 3.2.7, you can administer these external environments: ODBC, ESQL, .NET, Java, Perl, PHP.	<i>External Environments</i> on page 1189

Feature	Topics
Table administration – Perform table management tasks such as creating/deleting a base table and moving a table to another dbspace.	<i>Tables</i> on page 466
Table column administration – Add, modify, and delete table columns.	<i>Table Columns</i> on page 528
Table constraint administration – Manage column check, foreign key, table check, and unique constraints.	<i>Table Constraints</i> on page 556
Table index administration – Add, modify, delete, rebuild, validate, and move indexes on table columns.	<i>Table Indexes</i> on page 586
Table partition administration – Create, modify, delete, unpartition, merge, split, and move table partitions.	<i>Table Partitions</i> on page 617
Table trigger administration – Create, modify, and delete triggers on tables.	<i>Table Triggers</i> on page 606
View administration – Perform view management tasks such as creating a view and recompiling a materialized view.	<i>Views</i> on page 647
View trigger administration – Create, modify, and delete triggers on views.	<i>Triggers on Views</i> on page 679
LDAP server administration - Create, modify, and delete LDAP servers.	<i>LDAP Servers</i> on page 1133
Sequence Generator administration - Create, modify, and delete sequence generators.	<i>Sequence Generators</i> on page 788
Row-level Versioning (RLV) – Use the new RLV data store in your simplex database to perform row-level updates, inserts, and deletes, in real-time. When a table is enabled for storage in the RLV data store, multiple users can write to different rows of the table concurrently.	<i>Creating a Dbspace</i> on page 1148 <i>Creating a Dbfile</i> on page 1162 <i>Enabling RLV in a Table</i> on page 499
Remote Access – Access data from other data sources by creating Remote Server definitions, Proxy Tables, Remote Procedures and External Logins.	<i>Remote Servers</i> on page 437 <i>External Logins</i> on page 445 <i>Proxy Tables</i> on page 479 <i>Remote Procedures</i> on page 1254
Web service administration – Perform web service management tasks such as creating, modifying, and deleting web services.	<i>Web Services</i> on page 1273

Feature	Topics
Logical server administration – Logical server administration and monitoring and logical server policy administration have been enhanced.	<i>Logical Servers</i> on page 419 <i>Key Performance Indicators for SAP Sybase IQ</i> on page 307
Global transaction resiliency – Monitor the suspended, resumed, and rolled back status of INC (internode communication) connections for global transactions.	<i>Viewing Multiplex Connection Statistics</i> on page 374 <i>Key Performance Indicators for SAP Sybase IQ</i> on page 307
Spatial Data – Administer spatial reference systems, and spatial units of measure.	<i>Spatial Support</i> on page 802
Common Security Infrastructure – updates to the CSI improve SCC security and provide consistency across Sybase products.	—
Find a resource in the Administration Console – use new search and filter tools to locate objects of interest.	<i>Searching and Filtering Resources</i> on page 322
Login mappings – Map a Windows user profile or a Kerberos principal to an existing user in the database to maintain a single user ID for database connections, operating system, and network logins.	<i>Manage Login Mappings</i> on page 1109
Transport layer security – Configure transport layer security with RSA encryption in a multiplex environment.	<i>Editing the Multiplex Configuration File</i> on page 379
Data retrieval options – you can set thresholds to improve performance of the Administration Console.	<i>Configuring Retrieval Thresholds for the Administration Console</i> on page 118
View and filter logs, copy and paste from log snapshots.	<i>Using the SAP Sybase IQ Server and SCC Agent Logs</i> on page 1327
Message rows – the status of each object retrieval request is provided in a message row in the Administration Console. Message rows provide details for slow-responding requests, large result sets, and failed requests.	<i>Browsing and Managing Resources</i> on page 321
Administration scripts – The scripts <code>sync_server.sh</code> (.bat) and <code>stop_server.sh</code> (.bat) now require your login and password. For example <code>sync_server.sh <login> <password></code> .	<i>Generating Administration Scripts</i> on page 396

See also

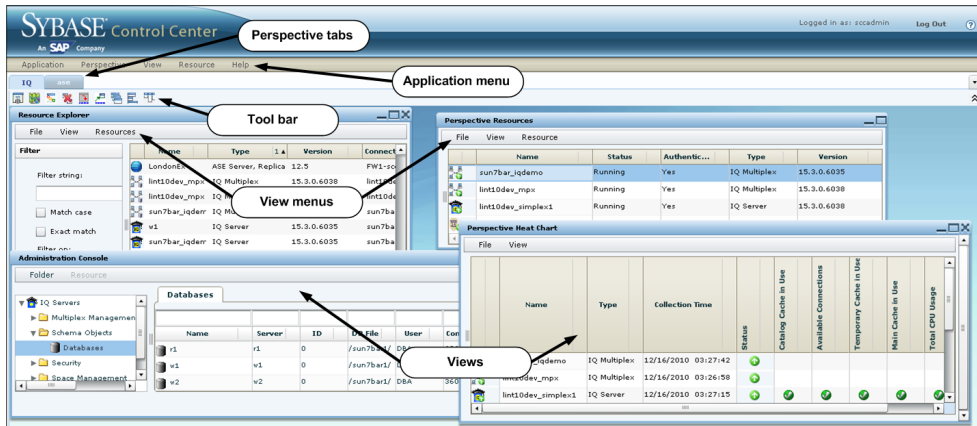
- *User Interface Overview* on page 4
- *Toolbar Icons* on page 5

- *Status Icons* on page 6
- *Common Display Options* on page 7
- *Keyboard Shortcuts* on page 10
- *Displaying the Versions of SCC Components* on page 11
- *Style and Syntax Conventions* on page 12
- *Accessibility Features* on page 14
- *Sybase Control Center Accessibility Information* on page 15

User Interface Overview

This illustration labels important elements of the Sybase Control Center user interface so you can identify them when they appear in other help topics.

Figure 1: Sybase Control Center User Interface












See also

- *New Features in Sybase Control Center for SAP Sybase IQ* on page 1
- *Toolbar Icons* on page 5
- *Status Icons* on page 6
- *Common Display Options* on page 7
- *Keyboard Shortcuts* on page 10
- *Displaying the Versions of SCC Components* on page 11
- *Style and Syntax Conventions* on page 12
- *Accessibility Features* on page 14
- *Sybase Control Center Accessibility Information* on page 15

Toolbar Icons

Describes the icons in the Sybase Control Center toolbar for launching and managing views.

Table 2. Toolbar Icons

Icon	Name	Description
	Show/Hide Perspective Resources View	Displays or minimizes the Perspective Resources view, which lists registered resources in this perspective.
	Launch Resource Explorer	Opens the resource explorer, which lists reachable resources (both registered and unregistered).
	Launch Heat Chart	Opens the perspective heat chart, which gives a status overview of the registered resources in this perspective.
	Close All Open Views	Closes all open and minimized views.
	Minimize All Open Views	Minimizes all open views.
	Restore All Minimized Views	Returns all minimized views to their original size.
	Cascade All Open Views	Arranges open views to overlap each other.
	Tile All Open Views Vertically	Arranges open views in a vertical manner.
	Tile All Open Views Horizontally	Arranges open views in a horizontal manner.

See also

- *New Features in Sybase Control Center for SAP Sybase IQ* on page 1
- *User Interface Overview* on page 4
- *Status Icons* on page 6
- *Common Display Options* on page 7
- *Keyboard Shortcuts* on page 10
- *Displaying the Versions of SCC Components* on page 11
- *Style and Syntax Conventions* on page 12

- *Accessibility Features* on page 14
- *Sybase Control Center Accessibility Information* on page 15

Status Icons







Sybase Control Center uses icons to indicate the status of resources and key performance indicators (KPIs).

Resource Status Icons in the Perspective Resources View and Heat Chart

Resource status icons indicate the condition of each resource in the heat chart. In addition, they are used as badges (small overlays) on server icons in both the heat chart and the Perspective Resources view. The Perspective Resources view also has a Status column that displays the same status as the badge in English text.

In the heat chart, hover the mouse over an icon in the Status column to display the status in English text.

Table 3. Resource Status Icons




Icon	Status	Description
	Running	Resource is up and running
	Pending	State is changing—check again
	Stopped	Resource has been shut down
	Warning	Resource has encountered a potentially harmful situation
	Error	Resource has encountered a serious problem
	Unknown	Resource is unreachable—state cannot be determined

KPI Status Icons in the Heat Chart

The heat chart uses KPI status icons to indicate the health of the KPIs it displays.

Hover the mouse over a KPI icon in any column to the right of the Status column to display the value of that KPI.

Table 4. KPI Status Icons

Icon	Status	Description
	Normal	Value of performance indicator is within the normal range
	Warning	Value of performance indicator is in the warning range
	Critical	Value of performance indicator is in the critical range

See also

- *New Features in Sybase Control Center for SAP Sybase IQ* on page 1
- *User Interface Overview* on page 4
- *Toolbar Icons* on page 5
- *Common Display Options* on page 7
- *Keyboard Shortcuts* on page 10
- *Displaying the Versions of SCC Components* on page 11
- *Style and Syntax Conventions* on page 12
- *Accessibility Features* on page 14
- *Sybase Control Center Accessibility Information* on page 15

Common Display Options

Use data display features to view resource status and to sort, search by resource name and type, and rearrange status information.

Column Options

The Perspective Resources view, Resource Explorer, Administration Console, Alert Monitor, heat chart, and other views in Sybase Control Center—including those in product modules—use a tabular grid format to display information about managed resources. You can use options provided by the grid format to sort and organize displayed data.












Table 5. Column Sorting Options

Sorting Option	Description
Simple column-based sorting	Click a column name to sort the table based on that column in ascending or descending order. The arrow in the column's sorting tab (to the right of the column name) points up when data is sorted in ascending order or down when data is sorted in descending order.

Sorting Option	Description
Reversing the order of a column-based sort	Click a column's sorting tab to reverse its sort from ascending to descending order or vice versa.
Nested sorting based on multiple columns	Click the column name for the primary sort. For subsidiary sorts, click the column's sorting tab. Choose the columns for subsidiary sorts in the order you want to apply them. After you click a sorting tab, it displays its sorting level (1 for the primary sort, 2 for the secondary sort, and so on).
Rearranging columns	Move columns by dragging and dropping them.

The figure below shows a table of servers sorted first by resource type; within type by software version; and within version by server name. The Type and Name columns sort in ascending order and the Version column sorts in descending order.

Figure 2: Resources sorted by type, version, and name

	Name	3 ▲	Type	1 ▲	Version	2 ▼
	mira8		ASE Server		15.0.2	
	mira9		ASE Server		15.0.2	
	LondonDR		ASE Server, Replication Only		12.5	
	LondonEx		ASE Server, Replication Only		12.5	
	NYEx		ASE Server, Replication Only		12.5	
	lint10dev_mpx		IQ Multiplex		15.3.0.6038	
	lint10dev_mpx		IQ Multiplex		15.3.0.6038	
	sun7bar_iqdemo		IQ Multiplex		15.3.0.6035	
	lamd6supt_r2		IQ Server		15.3.0.6038	
	lint10dev_cn		IQ Server		15.3.0.6038	
	lint10dev_r1		IQ Server		15.3.0.6038	

Filter by Column


The Administration Console provides a filtering field at the top of each column. Enter a filtering term to narrow the range of objects displayed. For example:

- Enter the name of a resource at the top of the Name column to display only that server, database, group, or other named object. The display reacts as you enter each character, so you might not need to enter the entire name.

- Enter a version number at the top of the Version column to display only resources running that software version.


You can filter on multiple columns; for example, in a listing of servers, use the Status column to display only running servers, then use the Version column to display servers using the desired software version. Delete the filtering terms to return to the original display. Filtering terms are not case sensitive.

Full Screen Mode

To increase the screen area available in Sybase Control Center for views and perspectives, click the  icon at the upper-right corner of the perspective area. Click the icon again to return to the original screen configuration.

Tip: To increase the screen area available to SCC, press **F11** to switch Internet Explorer or Firefox to full screen mode. Press **F11** again to return to the original browser configuration.

Maximize a Section of a View

Some areas within views have a square minimize/maximize icon () in the upper-right corner. Click the icon to expand that area to fill the entire view. Click the icon again to restore the area to its former size.

View Menu

The Perspective Resources view, the Resource Explorer, the Alert Monitor, and the heat chart each have a View menu. From the View menu, you can:

- Display the filtering tool for searches. (In the heat chart, the Filter option also displays the column selection tool.)
- Toggle between an icon view and a detail view of your resources (Perspective Resources view only)
- Refresh the display (Resource Explorer only)

Note: For these tasks, use the View menu in the view window, not the application-level View menu at the top of the SCC window.

See also

- *New Features in Sybase Control Center for SAP Sybase IQ* on page 1
- *User Interface Overview* on page 4
- *Toolbar Icons* on page 5
- *Status Icons* on page 6
- *Keyboard Shortcuts* on page 10
- *Displaying the Versions of SCC Components* on page 11
- *Style and Syntax Conventions* on page 12
- *Accessibility Features* on page 14
- *Sybase Control Center Accessibility Information* on page 15

Keyboard Shortcuts

Frequently used key sequences for the Sybase Control Center Web interface.

Key Sequence	Action
Ctrl-Alt-F12	Pull down the first menu in the topmost view or in the SCC menu bar. Repeat to toggle between the two first menus.
Ctrl-Alt-Shift-F12	Pull down the first menu (Application) in the SCC menu bar.
Space	Select the highlighted option—equivalent to clicking the mouse.
Escape	<ul style="list-style-type: none"> Release a drop-down menu Exit an editable cell or field Close a window
Arrow keys	<ul style="list-style-type: none"> Highlight the next list item or menu option in the indicated direction. For example, the down arrow highlights the next item down in a menu; the right arrow highlights an item in the menu to the right. In a tree hierarchy, the right arrow expands a node; the left arrow collapses it.
Tab	<ul style="list-style-type: none"> In a view, highlight the next item in the tab order. (Tab order progresses through the accessible fields in a left-to-right, top-to-bottom fashion, starting at the upper left.) In a two-pane view, jump from the tree hierarchy in the left pane to the right pane. In a view that includes a table or grid display, press Tab twice to highlight the table, then press the down-arrow to enter it.
Shift-Tab	<ul style="list-style-type: none"> In a view, highlight the previous item in the tab order. In a two-pane view, jump from the right pane back to the tree hierarchy in the left pane.
Home	Highlight the first item in the active view (or the active section of a view), for example the first row in a table.
End	Highlight the last item in the active view (or the active section of a view), for example the last row in a table.

Key Sequence	Action
In the SCC menu bar, View > Select > <your view>	Select an open view and bring it to the front.
Ctrl-Alt Arrow key	Move the selected view in the indicated direction.
Ctrl-Alt +	Increase the size of displayed text.
Ctrl-Alt -	Decrease the size of displayed text.
F11	Enable or disable the browser's full-screen mode.
In the SCC menu bar, Appli-cation > Display > Full Screen	Enable or disable Sybase Control Center's full-screen mode.

Sybase Control Center is built on Adobe Flex. For complete information about Adobe Flex keyboard shortcuts, see http://livedocs.adobe.com/flex/3/html/help.html?content=accessible_5.html.

See also

- *New Features in Sybase Control Center for SAP Sybase IQ* on page 1
- *User Interface Overview* on page 4
- *Toolbar Icons* on page 5
- *Status Icons* on page 6
- *Common Display Options* on page 7
- *Displaying the Versions of SCC Components* on page 11
- *Style and Syntax Conventions* on page 12
- *Accessibility Features* on page 14
- *Sybase Control Center Accessibility Information* on page 15

Displaying the Versions of SCC Components

View a list of components installed in Sybase Control Center and their versions.

Check the versions of the product modules in your SCC installation to determine whether your installation is up to date. SCC release bulletins list supported product module versions. You can find SCC release bulletins on the Product Documentation web site at <http://sybooks.sybase.com/sybooks/sybooks.xhtml?prodID=10680>

1. Log in to SCC and select **Help > About Sybase Control Center**.
2. Compare the versions of product modules (listed as management agent plug-ins) against the versions published in the most recent *Sybase Control Center Release Bulletin*.

See also

- *New Features in Sybase Control Center for SAP Sybase IQ* on page 1
- *User Interface Overview* on page 4
- *Toolbar Icons* on page 5
- *Status Icons* on page 6
- *Common Display Options* on page 7
- *Keyboard Shortcuts* on page 10
- *Style and Syntax Conventions* on page 12
- *Accessibility Features* on page 14
- *Sybase Control Center Accessibility Information* on page 15

Style and Syntax Conventions

A reference to the fonts and special characters used to express command syntax and to represent elements of system output and user input.

Table 6. Style Conventions

Key	Definition
monospaced(fixed-width)	<ul style="list-style-type: none">• SQL and program code• Commands to be entered exactly as shown• File names• Directory names
<i>italic monospaced</i>	In SQL or program code snippets, placeholders for user-specified values (see example below).
<i>italic</i>	<ul style="list-style-type: none">• File and variable names• Cross-references to other topics or documents• In text, placeholders for user-specified values (see example below)• Glossary terms in text

Key	Definition
bold sans serif	<ul style="list-style-type: none"> • Command, function, stored procedure, utility, class, and method names • Glossary entries (in the Glossary) • Menu option paths • In numbered task or procedure steps, user-interface (UI) elements that you click, such as buttons, check boxes, icons, and so on

A placeholder represents a system- or environment-specific value that you supply. For example:

```
installation directory\start.bat
```

where *installation directory* is where the application is installed.

Table 7. Syntax Conventions

Key	Definition
{ }	Curly braces indicate that you must choose at least one of the enclosed options. Do not type the braces when you enter the command.
[]	Brackets mean that choosing one or more of the enclosed options is optional. Do not type the brackets when you enter the command.
()	Parentheses are to be typed as part of the command.
	The vertical bar means you can select only one of the options shown.
,	The comma means you can choose as many of the options shown as you like, separating your choices with commas that you type as part of the command.
...	An ellipsis (three dots) means you may repeat the last unit as many times as you need. Do not include ellipses in the command.

See also

- *New Features in Sybase Control Center for SAP Sybase IQ* on page 1
- *User Interface Overview* on page 4
- *Toolbar Icons* on page 5
- *Status Icons* on page 6
- *Common Display Options* on page 7
- *Keyboard Shortcuts* on page 10
- *Displaying the Versions of SCC Components* on page 11
- *Accessibility Features* on page 14

- *Sybase Control Center Accessibility Information* on page 15

Accessibility Features

Accessibility ensures access to electronic information for all users, including those with disabilities.

Documentation for Sybase products is available in an HTML version that is designed for accessibility.

Vision impaired users can navigate through the online document with an adaptive technology such as a screen reader, or view it with a screen enlarger.

Sybase HTML documentation has been tested for compliance with accessibility requirements of Section 508 of the U.S Rehabilitation Act. Documents that comply with Section 508 generally also meet non-U.S. accessibility guidelines, such as the World Wide Web Consortium (W3C) guidelines for Web sites.

Note: You may need to configure your accessibility tool for optimal use. Some screen readers pronounce text based on its case; for example, they pronounce ALL UPPERCASE TEXT as initials, and MixedCase Text as words. You might find it helpful to configure your tool to announce syntax conventions. Consult the documentation for your tool.

For information about how Sybase supports accessibility, see the Sybase Accessibility site: <http://www.sybase.com/products/accessibility>. The site includes links to information about Section 508 and W3C standards.

You may find additional information about accessibility features in the product documentation.

See also

- *New Features in Sybase Control Center for SAP Sybase IQ* on page 1
- *User Interface Overview* on page 4
- *Toolbar Icons* on page 5
- *Status Icons* on page 6
- *Common Display Options* on page 7
- *Keyboard Shortcuts* on page 10
- *Displaying the Versions of SCC Components* on page 11
- *Style and Syntax Conventions* on page 12
- *Sybase Control Center Accessibility Information* on page 15

Sybase Control Center Accessibility Information

Sybase Control Center uses the Adobe Flex application.

For the most current information about Adobe Flex keyboard shortcuts, see http://livedocs.adobe.com/flex/3/html/help.html?content=accessible_5.html.

Note: To use Sybase Control Center effectively with versions of JAWS for Windows screen reading software before version 11, download and install the appropriate Adobe scripts. See <http://www.adobe.com/accessibility/products/flex/jaws.html>.

See also

- *New Features in Sybase Control Center for SAP Sybase IQ* on page 1
- *User Interface Overview* on page 4
- *Toolbar Icons* on page 5
- *Status Icons* on page 6
- *Common Display Options* on page 7
- *Keyboard Shortcuts* on page 10
- *Displaying the Versions of SCC Components* on page 11
- *Style and Syntax Conventions* on page 12
- *Accessibility Features* on page 14

Get Started

Set up Sybase® Control Center.

Quick Start for an Evaluation

(Optional) Get started using Sybase Control Center quickly if you do not need the full set of security features. This simplified process is suitable for a small-scale, temporary evaluation or proof-of-concept project, or for checking your installation.

Prerequisites

Install Sybase Control Center.

Task

Use these tasks to start Sybase Control Center, log in, register and authenticate a server, and monitor that server.

Note: After completing the tasks below and confirming that SCC is working, set up SCC for a production environment if you intend to continue using it.

1. *Registering the ODBC Driver in Windows*

In Windows, run scc.bat with administrative privileges to register the ODBC driver.

2. *Launching Sybase Control Center*

Use the scc command to start Sybase Control Center.

3. *Getting Started After Installing*

Perform postinstallation testing and configuration.

4. *Configuring SAP Sybase IQ Roles-Based Users for Monitoring*

For 16.0 and later databases, enable one or more SAP Sybase IQ role-based users or roles to authenticate an SAP Sybase IQ server with Sybase Control Center, create and populate the SCC_MONITOR role.

5. *Configuring SAP Sybase IQ Authority-Based Users for Monitoring*

For 15.3 and 15.4 databases, enable one or more SAP Sybase IQ authority-based users to authenticate an SAP Sybase IQ server with Sybase Control Center, create and populate the SCC_MONITOR group.

6. *Registering an SAP Sybase IQ Server*

Make Sybase Control Center aware of an SAP Sybase IQ resource (for example, a server that can be monitored) and its connection information by registering the resource.

7. *Authenticating a Login Account for a Managed Resource*

Specify the login account and password Sybase Control Center will use when it connects to your server or agent to collect monitoring data or manage the resource.

8. *Displaying Resource Availability: the Heat Chart*

Use the heat chart to view the status and availability of servers in the current perspective.

9. *Viewing Overview Statistics*

Display high-level statistics for the selected SAP Sybase IQ server.

10. *Viewing Multiplex Overview Statistics*

Display the overall health of the SAP Sybase IQ multiplex environment.

See also

- *Get Started in a Production Environment* on page 28

Registering the ODBC Driver in Windows

In Windows, run **scc.bat** with administrative privileges to register the ODBC driver.

When Sybase Control Center starts for the first time on a Windows machine, it registers its ODBC driver. Because the automatic registration of the ODBC driver edits the registry settings, you must execute **scc.bat** using elevated administrative privileges. If you launch for the first time without adequate privileges, Sybase Control Center generates an error and fails to start.

In Windows Vista, Windows 2008, and Windows 7, you must use the **Run as administrator** setting to launch Sybase Control Center even if you already have administrative privileges. This process is described below.

In other versions of Windows, you must be logged in as an administrator to start Sybase Control Center for the first time. You need not follow the steps below.

1. In Windows Vista, Windows 2008, or Windows 7, open the Command Prompt window with administrative privileges:
 - Select **Start > All Programs > Accessories**. Right-click **Command Prompt** and select **Run as administrator**.
 - Alternatively, enter **cmd** in the Start Menu search box and press **Shift+Ctrl+Enter**.
2. Run **scc.bat**.

Launching Sybase Control Center

Use the **scc** command to start Sybase Control Center.

Prerequisites

Install Adobe Flash Player in the browser you will use for Sybase Control Center.

Task

1. Start Sybase Control Center.

- Windows – navigate to `<install_location>\SCC-3_2\bin` and double-click **scc.bat**.
- UNIX – execute **scc.sh**.

Messages on the progress of the launch appear in a command window. When Sybase Control Center is running, the command window becomes the Sybase Control Center console; you can issue commands to get status information on SCC and its ports, plug-ins, and services.

2. Open a Web browser and enter `https://<hostname>:8283/scc`.

Getting Started After Installing

Perform postinstallation testing and configuration.

Prerequisites

Start Sybase Control Center.

Task

1. Install Adobe Flash Player 10.1 or later in the Web browser you will use to connect to Sybase Control Center.

Flash Player is a free plug-in. You can download the latest version from <http://get.adobe.com/flashplayer/>.

If Flash Player is already installed but you are not sure which version you have, go to the Adobe test site at <http://adobe.com/shockwave/welcome>. Click the link that says **Test your Adobe Flash Player installation**. The version information box on the next page that appears displays your Flash Player version.

2. To connect to Sybase Control Center, direct your browser to:

`https://<scc_server_hostname>:8283/scc`

Note: If you changed the default HTTPS port during installation, use the new port number instead of 8283.

3. If you see an error about the security certificate, add Sybase Control Center to your browser's trusted sites zone (Internet Explorer) or add a security exception (Firefox).
4. Log in.

Sybase Control Center provides a default login account, `sccadmin`, for initial configuration and setting up permanent authentication. The password is set during installation.

Note: The `sccadmin` account and the preconfigured user login module on which it is based are not intended for use in a production environment. Sybase recommends that you pass

authentication responsibility to your operating system or to LDAP, as described in the *Sybase Control Center > Get Started > Setting Up Security* section of the online help.

Sybase further recommends that you disable sccadmin as soon as you have set up and tested authentication, and that you change the password on the sccadmin account if you do not plan to set up and test authentication right away.

-
5. (Optional) Change the password or disable sccadmin—see the *Sybase Control Center Installation Guide* for instructions.

See also

- *Configuring SAP Sybase IQ Roles-Based Users for Monitoring* on page 129

Configuring SAP Sybase IQ Authority-Based Users for Monitoring

For 15.3 and 15.4 databases, enable one or more SAP Sybase IQ authority-based users to authenticate an SAP Sybase IQ server with Sybase Control Center, create and populate the SCC_MONITOR group.

Prerequisites

Log in to SAP Sybase IQ as a user with DBA authority.

Task

To monitor a resource with SCC, you must authenticate the resource as an SAP Sybase IQ user with DBA authority or membership in the SCC_MONITOR group.

Note: If you are performing a quick start, you need only authenticate your resource with Sybase Control Center using an SAP Sybase IQ account with DBA authority (such as DBA). You can skip the steps below until you do a complete production set-up of SCC.

The SCC_MONITOR script must be executed for each managed resource.

1. Using Interactive SQL or another SQL command tool, execute **scc_iq_monitor_privileges_setup.sql**, located in the directory SCC-3_2/plugins/IQMAP.
The script creates the SCC_MONITOR group and grants a set of permissions.
2. Assign one or more SAP Sybase IQ users or groups to the SCC_MONITOR group. You can do this by either of these methods:
 - Using Interactive SQL or another SQL command tool, execute **grant membership in group SCC_MONITOR to <user/group>**
 - In a user interface tool such as Sybase Control Center, add the user to the SCC_MONITOR group

See also

- *Configuring SAP Sybase IQ Roles-Based Users for Monitoring* on page 129

Registering an SAP Sybase IQ Server

Make Sybase Control Center aware of an SAP Sybase IQ resource (for example, a server that can be monitored) and its connection information by registering the resource.

Prerequisites

Ensure that the SAP Sybase IQ server does not have multiple databases. Sybase Control Center for SAP Sybase IQ supports a maximum of one database per server.

Task

1. In the Resource Explorer, select **Resources > Register**.
2. Specify:

Table 8. New Resource Type Details

Field	Description
Resource Name	(Required) Name of the resource to register. Enter the actual name of the server, including uppercase and lowercase letters. If the name registered in Sybase Control Center does not exactly match the server name, some monitoring functions may not work.
Resource Type	Select a resource type: <ul style="list-style-type: none"> • IQ Logical Server – register an SAP Sybase IQ logical server. • IQ Multiplex – register an SAP Sybase IQ multiplex server. • IQ Server – register an SAP Sybase IQ simplex server. Recommended. Can handle both simplex and multiplex servers.
Description	A brief description to help you identify the resource.

3. Click **Next**.
4. Specify the connection information for your resource:

Table 9. New Resource Connection Details

Field	Description
Host Name	(Required) Host name of the SAP Sybase IQ server.
IQ Port Number	(Required) Port number on server host.
Database	Name of the database.
Character Set	Character set to use for the connection.

Field	Description
Language	Language to use for the connection.
Logical Server	Name of the logical server. This only appears when registering a logical server.

5. (Optional) Enter a user name and password that SCC can use to authenticate with this resource to retrieve its software version. The credentials are used only for this purpose, then discarded.

If you prefer not to authenticate now, click **I do not want to supply authentication information**.

This step enables SCC to display the correct version information for the server before the server is formally authenticated (later in the configuration process).

6. Click **Next**.
7. (Optional) Click **Add this resource to the current perspective**. You must add a resource to a perspective (not necessarily the current perspective) before you can manage or monitor it.
8. (Optional) Click **Open the resource explorer to view this new resource**. (This option is not present when the Resource Explorer is open.)
The resource is added to the Resource Explorer even if you choose not to view it.
9. Click **Finish**.

Authenticating a Login Account for a Managed Resource

Specify the login account and password Sybase Control Center will use when it connects to your server or agent to collect monitoring data or manage the resource.

Perform this task for each resource registered with Sybase Control Center.

Note: You can also authenticate a server during administrative tasks like creating an alert or a collection job.

1. Connect a browser to Sybase Control Center and log in.
2. If the Perspective Resources view is not open, click the **Show/Hide Perspective Resources View** icon in the toolbar.
3. In the Perspective Resources view, select your resource and select **Resource > Authenticate** from the view menu.
4. Select **Use my current SCC login** or **Specify different credentials**.
5. If you chose **Specify different credentials**, enter the login and password for Sybase Control Center to use to connect to your resource.
6. If the selected resource is a Replication Server, also enter the RSSD user name and password.

7. Click **OK** to save and exit the dialog.

Displaying Resource Availability: the Heat Chart

Use the heat chart to view the status and availability of servers in the current perspective.

The heat chart displays the state of resources in your perspective—whether the resources are running, suspended, or down. In addition, the heat chart lists the type of each resource and provides statistical data, including the start time of the last data collection.

You can filter the resources that you want to see and search and sort the results by column. You can also select a resource and pull down its context menu to see monitoring and administrative options that vary based on the resource type.

Heat chart data is collected directly from managed servers, tagged with the date and time when it was collected, and stored in the Sybase Control Center repository.

1. From the application menu bar, select **View > Open > Heat Chart**.
2. (Optional) To display information about the status represented by an icon in the chart, hover the mouse over the icon.
 - Status column – icon tooltips describe the status of the resource (Running or Stopped, for example).
 - All columns to the right of Status – icon tooltips give the value of the KPI listed at the top of the column.
3. (Optional) To display tools for filtering (narrowing the list of resources in the heat chart) or changing the columns, select **View > Filter** from the Perspective Heat Chart menu bar. The Filter and Column tools appear in the left pane.
4. (Optional) To use filtering, select **View > Filter** from the view's menu bar and enter a search term in the **Filter string** field.

The search term can be any string that appears in the tabular portion of the heat chart, such as the name, or part of the name, of a server or a resource type (ASE Server, for example).
5. (Optional) Select a filtering setting:
 - **Match case** – search for resources whose displayed data includes the search term, including uppercase and lowercase letters; or
 - **Exact match** – search for resources whose displayed data includes an item identical to the search term.
6. (Optional) Select a column from the **Filter on** list to restrict your search to that column.
7. (Optional) Click **Columns** to customize your heat chart.
8. (Optional) Unselect any column that should not appear in your heat chart.
9. (Optional) Click the sorting arrow in the column headers to sort the column values in either ascending or descending order.
10. (Optional) Click the resource's row and pull down the menu to the right of the resource name to view options for the selected resource.

11. (Optional) To resize the Filter and Columns tools pane, move your mouse over the border between the tools pane and the resource table. When the mouse cursor changes to a resize icon, click and drag the border to the left or the right.
12. (Optional) To hide the Filter and Columns tools, unselect **View > Filter**.

Viewing Overview Statistics

Display high-level statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Overview**.
3. Select the tab for the required information.

Note: Click a column header to sort the data by that column.

To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Tab	Description
Server	<p>State – current status of the server. Valid states include:</p> <ul style="list-style-type: none">• Unknown• Stopped• Running <p>Host – host name where the server is running.</p> <p>Port – port number where the server is running.</p> <p>Server name – name of the server.</p> <p>Database – name of the SAP Sybase IQ database.</p> <p>Server type – type of server the database is on. Server types include Single Server, Coordinator, Reader, and Writer.</p> <p>Server version – version of the SAP Sybase IQ server.</p> <p>Platform – operating system running on the server host.</p>

Tab	Description
Activities	<p>CPU total usage (%) – total CPU usage percentage, including both system and user usage.</p> <p>Active connections – total number of active connections, including user and internode communication connections.</p> <p>Connections available – number of connections available for users and internode communication connections.</p> <p>Active requests – number of active requests on the server.</p> <p>IQ threads in use – number of threads being used by the SAP Sybase IQ server.</p> <p>Active transactions – number of active transactions.</p> <p>Number of committed transactions – number of committed transactions.</p> <p>Oldest transaction (minutes) – elapsed age, in minutes, of the oldest transaction.</p>
Caches	<p>Catalog cache reads (per second) – number of catalog cache page lookups per second.</p> <p>Main cache size (MB) – size of the main cache, in megabytes.</p> <p>Temp cache size (MB) – size of the temporary cache, in megabytes.</p> <p>Remaining heap size (MB) – size of the remaining heap allocation, in megabytes.</p>
Version usage	<p>Number of committed versions – the number of table versions in the server.</p> <p>Total version space used (MB) – total space consumed by all the table versions.</p> <p>Oldest version ID – the oldest version identifier on the server.</p> <p>Number of active versions – total number of active write table versions on the server.</p> <p>Total active version space created (MB) – amount of data created by active write transactions.</p> <p>Total active version space to be destroyed (MB) – amount of data destroyed by active write transactions. If these transactions commit, the destroyed data becomes an old version and is eventually dropped. If the transactions roll back, the created data is released.</p>
Details	<p>Server full version – version of the IQ server software, including the date and time.</p> <p>Platform version – version of the operating system installed on the server host.</p>
Alerts	<p>Any alerts for the selected server. While the monitor is open, alerts are displayed as they are created.</p>

Tab	Description
CPU history chart	Percentage of total CPU usage over a period of time.
IQ memory chart	Allocation of the IQ memory between the main cache, temporary cache, and remaining heap.
Disk usage chart	Available and used space for the main and temporary stores.

Viewing Multiplex Overview Statistics

Display the overall health of the SAP Sybase IQ multiplex environment.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Overview**.
3. Select the tab for the required information.

Note: Click a column header to sort the data by that column.

To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
------	-------------

Area	Description
Multiplex tab > Servers	<p>Server – name of the server.</p> <p>Host – host name where the server is running.</p> <p>Port – port number where the server is running.</p> <p>State – current state of the server. Valid states include:</p> <ul style="list-style-type: none"> • Unknown • Stopped • Running <p>Role – role the server plays in the multiplex configuration. Roles include:</p> <ul style="list-style-type: none"> • Coordinator • Reader • Writer <p>Status – current status of the server in the multiplex. Valid states include:</p> <ul style="list-style-type: none"> • Included • Excluded
Multiplex tab > CPU History	Percentage of total CPU usage over a period of time for each server. The legend below the chart identifies the colored line associated with each server.
Multiplex tab > IQ Memory	Allocation of the IQ memory between the main cache and temporary cache for each server in the multiplex.
Disk Usage tab	Available and used space for the main store and temporary store on each server in the multiplex.
Version Usage tab > Statistics	<p>Number of committed versions – the number of table versions in the servers.</p> <p>Total version space used (MB) – total space consumed by all the table versions.</p> <p>Oldest version ID – the oldest table version identifier on the server.</p> <p>Number of active versions – total number of active write table versions on the servers.</p> <p>Total active version space created (MB) – amount of data created by active write transactions.</p> <p>Total active version space to be destroyed (MB) – amount of data destroyed by active write transactions. If these transactions commit, the destroyed data becomes an old version and is eventually dropped. If the transactions roll back, the created data is released.</p>

Area	Description
Version Usage tab > Multiplex Version Usage	<p>Version ID – the table version identifier.</p> <p>Server name – the name of the server where the table version exists.</p> <p>Connection ID – the connection ID using this table version.</p> <p>WasReported – indicates whether the server has received usage information for this table version.</p> <p>MinKBRelease – the minimum amount of space returned once this table version is no longer in use.</p> <p>MaxKBRelease – the maximum amount of space returned once this table version is no longer in use.</p>
Alerts	Any alerts for the selected multiplex. While the monitor is open, alerts are displayed as they are created.

Get Started in a Production Environment

Perform a complete setup of Sybase Control Center, including configuration of user authentication and other one-time set-up tasks.

Prerequisites

Install Sybase Control Center and complete the follow-up tasks described in the *Sybase Control Center Installation Guide*.

1. *Deploying an Instance from a Shared Disk Installation*

(Optional) Create a Sybase Control Center server or agent from an installation on a shared disk.

2. *Starting and Stopping Sybase Control Center in Windows*

There are several ways to start and stop Sybase Control Center or the SCC agent. You can start manually, which is useful for testing and troubleshooting, or set the service to start automatically and to restart in case of failure.

3. *Starting and Stopping Sybase Control Center in UNIX*

You can start Sybase Control Center or the SCC agent manually, which is useful for testing and troubleshooting, or you can set up a service to start automatically and to restart in case of failure.

4. *Configuring Memory Usage*

(Optional) Determine whether you need to configure how much memory Sybase Control Center uses, and if so which configuration method to use.

5. *Logging in to Sybase Control Center*

Enter the Sybase Control Center Web console.

6. *Setting Up Security*

Configure login authentication and map roles.

7. *Configuring the E-mail Server*

(Optional) Specify the e-mail server for Sybase Control Center to use to send e-mail alert notifications.

8. *Configuring the Automatic Logout Timer*

(Optional) Set Sybase Control Center to end login sessions when users are inactive for too long.

9. *User Authorization*

The authorization mechanism in Sybase Control Center employs login accounts and task-based roles.

10. *Configure Sybase Control Center*

Configure Sybase Control Center for SAP Sybase IQ.

Deploying an Instance from a Shared Disk Installation

(Optional) Create a Sybase Control Center server or agent from an installation on a shared disk.

Prerequisites

- Install Sybase Control Center on a shared disk.
- Enable shared-disk mode.

Task

1. Log in to the host on which you plan to run the SCC server or agent.

Note: You can create an instance on one host and run it on another host, but doing so interferes with the predeployment checks run by **sccinstance**. Such a deployment might generate errors (port conflicts, for example). If you are confident that the errors are caused by problems that will not be present on the host where you plan to run the instance, use the **-force** option to create the instance.

2. Change to `SCC-3_2/bin`.
3. Create the instance as an SCC agent if you plan to run a managed server on this host. Create the instance as an SCC server if you plan to manage other Sybase servers from this host.

To create an SCC agent called Boston-agent and configure it to run as a Windows service:

```
sccinstance -create -agent -instance Boston-agent -service
```

To create an SCC server called Boston and configure it to run as a Windows service:

Get Started

```
sccinstance -create -server -instance Boston -service
```

On UNIX systems, omit the **-service** option.

4. If other SCC instances will run on this host, change the port assignments for the new instance. Change the instance names and port values in the sample commands to suit your environment, but take care to specify ports that are not in use by another SCC instance or any other application or server.

This command changes the port assignments for an SCC agent called myagent:

```
sccinstance -refresh -instance myagent -portconfig  
rmi=8888,jiniHttp=9093,jiniRmi=9096,tds=9997
```

This command changes the port assignments for an SCC server called myserver:

```
sccinstance -refresh -server -instance myserver -portconfig  
rmi=8889,db=3640,  
http=7072,https=7073,jiniHttp=9094,jiniRmi=9097,msg=2002,tds=9996
```

5. (Optional) List the instances deployed from this installation:

```
sccinstance -list
```

6. (Optional) If you are setting up an instance in UNIX, configure it to run as a service. See *Starting and Stopping Sybase Control Center in UNIX*.

Next

When you manage and maintain instances, keep in mind that the directory structure for instances is different from that of singleton installations. In file paths in SCC help, replace SCC-3_2 or <scc-install-directory> with SCC-3_2/instances/<instance-name>.

For example, the path to the log directory, SCC-3_2/log, becomes this for an instance called kalamazoo:

```
SCC-3_2/instances/kalamazoo/log
```

See also

- *Starting and Stopping Sybase Control Center in Windows* on page 36

Enabling and Disabling Shared-Disk Mode

Turn on or turn off shared-disk mode, which allows you to run multiple Sybase Control Center agents and servers from a single installation on a shared disk.

Prerequisites

Install Sybase Control Center on a shared disk. See the *Sybase Control Center Installation Guide*.

Task

Shared-disk mode affects the entire installation; do not enable or disable individual instances.

Disabling shared-disk mode leaves the instances' file systems intact under <SCC-install-directory>/instances, but the instances cannot run. If you reenables, the instances are able to run again.

1. Change to SCC-3_2/bin.
2. Enable or disable shared disk mode.

To enable shared disk mode:

```
sccinstance -enable
```

To disable shared disk mode:

```
sccinstance -disable
```

Shared-Disk Mode

Shared-disk mode lets you run multiple Sybase Control Center instances—SCC servers, SCC agents, or a mixture of the two—from a single installation of the product.

The shared-disk capability enables SCC servers or agents on the installation host or on remote hosts to access and execute from the same installation. This feature is especially useful if you plan to use SCC to manage Adaptive Server® clusters, SAP Sybase ESP clusters, or SAP Sybase IQ multiplexes.

After installing SCC on a shared disk, use the **sccinstance** command to enable shared-disk mode and deploy instances. **sccinstance** copies the files needed for the instance into a new directory structure. The path takes the form <SCC-install-directory>/instances/<instance-name> (for example, SCC-3_2/instances/SCCserver-1).

You can specify a name for each instance. If you do not supply a name, the instance name defaults to the host name.

An instance runs on the host on which you start it. When shared-disk mode is enabled, SCC servers and agents run out of the SCC-3_2/instances subdirectories, not from the base file system.

In shared-disk mode, changes made to configuration files in the base file system (everything under SCC-3_2 except the SCC-3_2/instances branch) are copied to any instance deployed thereafter. Previously deployed instances are not affected.

Use **sccinstance** to deploy, remove, refresh, or convert an instance; to configure an instance's ports; and to configure a Windows instance to run as a service. Perform other tasks, including configuring a UNIX instance to run as a service, and all other configuration, using the tools and procedures documented for all installations. Use tools provided by the UI wherever possible. When you must edit a file to change the configuration of an instance (for role

Get Started

mapping, for example), edit the copy of the file stored under <SCC-install-directory>/instances/<instance-name>.

sccinstance Command

Use **sccinstance.bat** (Windows) or **sccinstance** (UNIX) to deploy an instance of Sybase Control Center from a shared-disk installation or to manage existing instances.

You can run multiple instances of Sybase Control Center, including SCC servers, SCC agents, or a mixture of the two, from a single installation on a shared disk.

Syntax

```
sccinstance[.bat]
[-agent]
[-c | -create]
[-d | -debug]
[-disable]
[-enable]
[-f | -force]
[-h | -help]
[-host host-name]
[-i | -instance [instance-name]]
[-l | -list]
[-plugins {plugin-ID,plugin-ID,...}]
[-portconfig {port-name=port-number,port-name=port-number, ...}]
[-refresh]
[-r | -remove]
[-s | -server]
[-service]
[-silent]
```

Parameters

- **-agent** – use with **-create** or **-refresh** to create or refresh an SCC agent. In a **-create** or **-refresh** command, **-agent** is the default, so you can omit it.
- **-create** – deploy a new instance. Use alone or with **-agent** to create an agent instance, or with **-server** to create a server instance.
- **-d | debug** – display debugging messages with the output of this command.
- **-disable** – turn off shared-disk mode for this installation. Generates an error if any instance is running.
- **-enable** – turn on shared-disk mode for this installation. Shared-disk mode is required if you intend to run more than one server or agent from a single installation of SCC.
- **-f | -force** – execute **sccinstance** even if there are potential conflicts, such as port clashes or a running SCC process. Sybase does not recommend using **-force** to remove or refresh a running instance in a Windows environment.
- **-h | --help** – display help and usage information for the **sccinstance** command.
- **-host *host-name*** – specify the host for this instance. Use with **-create**; required only when the instance name does not match the name of the host on which this instance will run. (The

instance name defaults to the name of the current host unless you use **-instance** to specify another name.)

- **-instance** [*instance-name*] – specify an instance. Use with **-create**, **-remove**, or **-refresh**, or use alone to display the instance’s status. You can omit **-instance** when you are addressing the only SCC instance or the only instance of the specified type (server or agent) on the current host.

sccinstance assumes that the host name is the same as the instance name unless you use **-host** to specify a different host name.

- **-l** | **-list** – display a list of all instances deployed from this SCC installation.
- **-plugins** {*plugin-ID,plugin-ID,...*} – specify one or more product module plug-ins for this instance. An alternative to **-agent** and **-server**, **-plugins** is primarily for use by the SCC installation program. Use with **-create** or **-refresh**. Use commas to separate plug-in names.
- **-portconfig** {*port-name=port-number, port-name=port-number, ...*} – assign ports to services for this instance. Use only with **-create** or **-refresh**. For the *port-name* value, use a port name from the table below. If you plan to run more than one SCC instance on a host machine, you must reassign all the ports for every instance after the first.

Port information:

Port Name	Description	Service Names	Property Names	Default Port
db	Database port Present on SCC server	SccSADataserver Messaging Alert Scheduler	com.sybase.asa.server.port messaging.db.port alert.database.port org.quartz.data-Source.ASA.URL	3638
http	Web HTTP port Present on SCC server	EmbeddedWebCon- tainer	http.port	8282
https	Web HTTPS (secure HTTP) port Present on SCC server	EmbeddedWebCon- tainer	https.port	8283
jiniHttp	JINI HTTP server Present on SCC server and SCC agent	Jini	httpPort	9092
jiniR- mid	JINI remote method in- vocation daemon Present on SCC server and SCC agent	Jini	rmidPort	9095

Port Name	Description	Service Names	Property Names	Default Port
msg	Messaging port Present on SCC server	Messaging	messaging.port	2000
rmi	RMI port Present on SCC server and SCC agent	RMI	port	9999
tds	Tabular Data Stream™ port (used to communicate with other Sybase products) Present on SCC server and SCC agent	Tds	tdsPort	9998

- **-refresh** – recopy all the files that make up this instance (Windows) or all this instance's services and plug-ins (UNIX). Refreshing preserves any service or plug-in configuration in the deployed instance.

You can also use **-refresh** to convert a server to an agent or an agent to a server (see the examples). Files are removed or added to change the function of the instance. Use alone or with **-agent** to refresh an agent instance, or with **-server** to refresh a server instance. Generates an error if the instance is running.

- **-r | -remove** – delete an instance. Use alone or with **-instance**. Generates an error if the instance is running. You cannot restore a removed instance.
- **-s | -server** – use with **-create** or **-refresh** to create or refresh an SCC server, including any product modules available.
- **-service** – use with **-create** or **-remove** to create or remove a Windows service for this instance. You must be logged in to Windows as an administrator to use this option.
- **-silent** – suppress the output of **sccinstance**.

Examples

- **Deploy an SCC server instance** – enables shared-disk mode, deploys a server called Boston with a Windows service on the current host, and starts the Windows service:

```
sccinstance -enable
sccinstance -create -server -instance Boston -service
net start "Sybase Control Center 3.2.3 (Boston)"
```

Note: To create the service, you must log in to Windows as an administrator.

- **Deploy an SCC agent instance** – deploys an SCC agent on this host and configures a Windows service for it. The **-agent** option, because it is the default, is not required—the command does exactly the same thing without it.

```
sccinstance -create -agent -service
```

or

```
sccinstance -create -service
```

- **Deploy a server instance and reassign ports** – deploys the server on this host and configures nondefault RMI, HTTP, and HTTPS ports.

```
sccinstance -create -server -portconfig  
rmi=8888,http=7070,https=7071
```

- **Deploy two instances on the same host** – creates two agent instances on the host fireball. The first command does not need the **-host** option because the instance name is the same as the host name.

```
sccinstance -create -agent -instance fireball -portconfig rmi=9991  
sccinstance -create -agent -instance fireball2 -host fireball  
-portconfig rmi=9992
```

Note: In a production environment, Sybase recommends that you deploy no more than one SCC instance of each type (one server and one agent) on the same host.

- **Refresh a server instance or convert an agent to a server** – refreshes the server on this host. If the instance on this host is an SCC agent, refreshing it as an SCC server converts it into a server.

```
sccinstance -refresh -server
```

- **Refresh an agent instance or convert a server to an agent** – refreshes the instance named kalamazoo. If kalamazoo is a server, refreshing it as an SCC agent converts it into an agent.

```
sccinstance -refresh -agent -instance kalamazoo
```

- **Remove a server instance** – removes the instance named porcupine if it is not running:

```
sccinstance -remove -instance porcupine
```

- **Display status** – displays the status of the instance on this host:

```
sccinstance
```

- **List all instances** – displays a list of all SCC server and agent instances deployed from this SCC installation:

```
sccinstance -list
```

- **Scenario: Remove an instance by force** – suppose you have inadvertently deployed two SCC agent instances on the same host:

```
$ sccinstance -list  
2 SCC instances deployed:  
SCC instance node1 deployed in agent mode for host node1 RMI port  
9999  
SCC instance node2 deployed in agent mode for host node2 RMI port  
9999
```

Get Started

Both instances use the same RMI port. You must either reassign ports for one instance or remove it. But you get an error if you try remove an instance when another instance is running on the same host:

```
$ sccinstance -instance node2 -remove
[ERROR] Command execution failed.
[ERROR] SCC instance node2 could not be removed because it is
running. Shut
down the SCC before removing the instance.
```

Use the **-force** option to override the error and force the removal of the second agent instance:

```
$ sccinstance -instance node2 -remove -force
Removing SCC instance node2 ...
SCC instance node2 was successfully removed.
```

Permissions

sccinstance permission defaults to all users, except as noted for certain parameters.

Starting and Stopping Sybase Control Center in Windows

There are several ways to start and stop Sybase Control Center or the SCC agent. You can start manually, which is useful for testing and troubleshooting, or set the service to start automatically and to restart in case of failure.

This topic applies to both Sybase Control Center (the server, which includes the management UI) and the Sybase Control Center agent that runs on each product server managed by SCC. When you install SCC and the SCC agent in the same directory by selecting both options in the installer, you start and stop them together—by executing a single command or controlling a single service. This topic applies both to singleton installations (which do not use a shared disk) and to instances of SCC agents and servers running from a shared disk.

If you run Sybase Control Center or the SCC agent manually, you must issue a command every time you start or shut down. If you run as a service (which is recommended), you can configure the service to start and restart automatically. These are the options:

- Use the **scc.bat** command to start Sybase Control Center or the SCC agent manually. The command gives you access to the Sybase Control Center console, which you can use to shut down and to display information about services, ports, system properties, and environment variables. You can also use **scc.bat** to change the logging level for troubleshooting purposes. Using **scc.bat** prevents you from taking advantage of the automatic start and restart features available to services.
- Use the Services list under the Windows Control Panel to start, stop, and configure the Sybase Control Center service for an SCC server or agent.
- Use the **net start** and **net stop** commands. This is another way to run Sybase Control Center or the SCC agent as a service.

Note: To start an SCC agent or server as a service:

- In a singleton installation, you must have selected **Yes** in the installer to install the agent or server as a service.
 - In a shared disk installation, the agent or server must have been deployed using the **-service** option of the **sccinstance** command.
-

In a singleton installation, the installer lets you start Sybase Control Center or the SCC agent as a service and configures the service to restart automatically. Before starting, check the Windows Services list for a Sybase Control Center service.

Here are the steps for each starting and stopping option:

- **Start Sybase Control Center, the SCC agent, or both when they are installed together:**

- (Skip this step for the SCC agent.) If you are starting Sybase Control Center for the first time in Windows Vista, Windows 2008, or Windows 7, set the **Run as Administrator** option on the command prompt so that Sybase Control Center can register its ODBC driver. (This is necessary even if you are logged in as an administrator.)
- Enter the **scc** command.

For a singleton installation:

```
%SYBASE%\SCC-3_2\bin\scc.bat
```

For an instance:

```
%SYBASE%\SCC-3_2\bin\scc.bat -instance <instance-name>
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

- **Stop Sybase Control Center, the SCC agent, or both when they are installed together:**

- Enter the **scc --stop** command.

For a singleton installation:

```
%SYBASE%\SCC-3_2\bin\scc.bat --stop
```

For an instance:

```
%SYBASE%\SCC-3_2\bin\scc.bat --stop -instance <instance-name>
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

Note: You can also enter **shutdown** at the **scc-console>** prompt.

- **Start or stop from the Windows Control Panel; configure automatic start and restart:**

- a) Open the Windows Control Panel.
- b) Select **Administrative Tools > Services**.
- c) Locate “Sybase Control Center” in the Services list. It may be followed by a release number; if the service is for an instance, it is also followed by the instance name. Service names do not distinguish between agents and servers. If the service is running, the Status column displays “Started.”
- d) To start or stop the service, right-click the **Sybase Control Center** entry in the Services list and choose **Start** or **Stop**.
- e) To configure automatic starting, double-click the service.
- f) To set the service to automatically start when the machine starts, change the **Startup type** to Automatic.
- g) To restart the service in case of failure, choose the **Recovery** tab and change the First, Second, and Subsequent failures to Restart Service.
- h) Click **Apply** to save the modifications and close the dialog.
- **Start or stop the Sybase Control Center service (controlling Sybase Control Center, the SCC agent, or both) from the Windows command line:**
 - a) To start the service, enter the **net start** command.

For a singleton installation:

```
net start "sybase control center 3.2.8"
```

```
The Sybase Control Center 3.2.8 service is starting.....
The Sybase Control Center 3.2.8 service was started
successfully.
```

For an instance, include the instance name (Boston-1 in this example) in parentheses:

```
net start "sybase control center 3.2.8 (Boston-1)"
```

```
The Sybase Control Center 3.2.8 (Boston-1) service is
starting.....
The Sybase Control Center 3.2.8 (Boston-1) service was
started successfully.
```

- b) To stop the service, enter the **net stop** command.

For a singleton installation:

```
net stop "sybase control center 3.2.8"
```

```
The Sybase Control Center 3.2.8 service is stopping.....
The Sybase Control Center 3.2.8 service was stopped
successfully.
```

For an instance, include the instance name (Boston-1 in this example) in parentheses:

```
net stop "sybase control center 3.2.8 (Boston-1)"
```

```
The Sybase Control Center 3.2.8 (Boston-1) service is
stopping.....
```

```
The Sybase Control Center 3.2.8 (Boston-1) service was
stopped successfully.
```

See also

- *Deploying an Instance from a Shared Disk Installation* on page 29

Starting and Stopping Sybase Control Center in UNIX

You can start Sybase Control Center or the SCC agent manually, which is useful for testing and troubleshooting, or you can set up a service to start automatically and to restart in case of failure.

This topic applies to both Sybase Control Center (the server, which includes the management UI) and the Sybase Control Center agent that runs on each product server managed by SCC.. When you install SCC and the SCC agent in the same directory by selecting both options in the installer, you start and stop them together—by executing a single command or controlling a single service. This topic applies to both singleton installations (which do not use a shared disk) and instances of SCC agents and servers running from a shared disk.

If you start Sybase Control Center or the SCC agent manually, you must issue a command every time you start or shut down. If you run as a service (which is recommended), you can configure the service to start and restart automatically. These are the options:

- Use the **scc.sh** script to start Sybase Control Center or the SCC agent manually. You can either:
 - Run **scc.sh** in the foreground to get access to the Sybase Control Center console, which you can use to shut down and to display information about services, ports, system properties, and environment variables.
 - Run **scc.sh** in the background to suppress the console.

You can use **scc.sh** to run Sybase Control Center at a nondefault logging level for troubleshooting. When you start manually with **scc.sh**, you cannot take advantage of the automatic start and restart features available to services.

- Use the **sccd** script to configure a service that starts Sybase Control Center or the SCC agent automatically.

Here are the steps for each starting and stopping option:

- **Before you start Sybase Control Center or the SCC agent for the first time, set environment variables.** Do this only once.
 - a) Change to the Sybase directory (the parent of the Sybase Control Center installation directory).
 - b) Execute one of the following to set environment variables.

Bourne shell:

```
. SYBASE.sh
```

C shell:

```
source SYBASE.csh
```

- **Run Sybase Control Center or the SCC agent (or both, when they are installed together) in the foreground.**

Running in the foreground is a method of manually starting; you must issue commands to stop and restart Sybase Control Center or the SCC agent.

- a) To start Sybase Control Center or the SCC agent and drop into the console when the start-up sequence is finished, enter the **scc** command.

For a singleton installation:

```
$SYBASE/SCC-3_2/bin/scc.sh
```

For an instance:

```
$SYBASE/SCC-3_2/bin/scc.sh -instance <instance-name>
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

- **Run Sybase Control Center or the SCC agent (or both, when they are installed together) in the background.**

You can use **nohup**, **&**, and **>** to run Sybase Control Center or the SCC agent in the background, redirect output and system error to a file, and suppress the SCC console. Running in the background is a method of manually starting; you must issue commands to stop and restart Sybase Control Center or the SCC agent.

- a) Execute a command similar to the sample below that matches your shell. Both sample commands direct output to the file `scc-console.out`. If the output file already exists, you might need to use additional shell operators to append to or truncate the file.

Bourne shell (sh) or Bash

For a singleton installation:

```
nohup ./scc.sh 2>&1 > scc-console.out &
```

For an instance:

```
nohup ./scc.sh -instance <instance-name> 2>&1 > scc-console-  
your-instance.out &
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

C shell

For a singleton installation:

```
nohup ./scc.sh >& scc-console.out &
```

For an instance:

```
nohup ./scc.sh -instance <instance-name> >& scc-console.out &
```


You can omit the **-instance** option if the instance's name is the same as its host name (the default).

- **Shut down Sybase Control Center or the SCC agent (or both, when they are installed together) .**

a) To shut down from the `scc-console>` prompt, enter:

```
shutdown
```

Warning! Do not enter **shutdown** at a UNIX prompt; it shuts down the operating system.

To shut down from the UNIX command line, enter the **scc --stop** command.

For a singleton installation:

```
$SYBASE/SCC-3_2/bin/scc.sh --stop
```

For an instance:

```
$SYBASE/SCC-3_2/bin/scc.sh --stop -instance <instance-name>
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

- **Configure Sybase Control Center or the SCC agent to run as a service.**

A UNIX service is a daemon process that starts automatically after the machine is started and runs in the background. UNIX installations of Sybase Control Center include a shell script, **sccd**, which you can use to configure the Sybase Control Center service. (Some UNIX platforms supply tools that make service configuration easier; Linux **chkconfig** is an example.)

Note: Sybase recommends that if you are not familiar with setting up services in UNIX, you delegate this task to a system administrator or consult the system administration documentation for your UNIX platform.

a) Copy `$SYBASE/SCC-3_2/bin/sccd` into this directory:

- AIX (SCC agent only): `/etc/rc.d/init.d`
- HP-UX (SCC agent only): `/sbin/init.d`
- All other platforms: `/etc/init.d`

b) Open `sccd` and make these changes:

- Change the line that sets the SYBASE variable to the location of your Sybase installation (that is, the parent of `SCC-3_2`, the Sybase Control Center installation directory). By default, this directory is called `Sybase`.
- If you are not using shared-disk mode, or you are using shared-disk mode to run a single instance whose name is the same as the host name, skip to step 5.c on page 42 or step 5.d on page 42.

- If you are using shared-disk mode to run a single instance whose name is not the host name, or to run multiple instances on the same host, add the instance name to the script name. Change:

```
SCRIPT_NAME=scc.sh
```

to:

```
SCRIPT_NAME="scc.sh -instance <instance-name>"
```

- If you are using shared-disk mode to run multiple instances on the same host, append the instance name to the name of the output log file. Change:

```
./${SCRIPT_NAME} --start 2>&1 >> ${SCC_HOME}/log/scc-  
service.out &
```

to:

```
./${SCRIPT_NAME} --start 2>&1 >> ${SCC_HOME}/log/scc-  
service_<instance-name>.out &
```

- If you are using shared-disk mode to run multiple instances on the same host, save a copy of the `sccd` script for each instance, giving each copy a unique name. In each copy, add the instance name to the script name and append the instance name to the output log file name as described above. Perform the remaining steps in this procedure for each copy of `sccd`.

- c) In Linux, configure the service to run in run levels 2, 3, 4, and 5:

```
/usr/sbin/chkconfig --add sccd  
/usr/sbin/chkconfig --level 2345 sccd
```

You can test the `sccd` script with `/usr/sbin/service sccd status`. (The **service** command accepts these options: **start** | **stop** | **status** | **restart**.)

- d) On non-Linux platforms, locate this directory:

- AIX (SCC agent only): `/etc/rc.d/rc<X>.d`
- HP-UX (SCC agent only): `/sbin/rc<X>.d`
- Solaris: `/etc/rc<X>.d`

where `<X>` is the run level (for example, 3). Make two soft links in the directory for your platform and set the links to point to:

- AIX (SCC agent only):
`/etc/rc.d/init.d/sccd: S90sccd` and
`/etc/rc.d/init.d/sccd: K10sccd`
- HP-UX (SCC agent only):
`/sbin/init.d/sccd: S90sccd` and
`/sbin/init.d/sccd: K10sccd`
- Solaris:
`/etc/init.d/sccd: S90sccd` and
`/etc/init.d/sccd: K10sccd`

The `S90sccd` link starts the service and the `K10sccd` link stops the service. The two-digit numbers in the links indicate the start and stop priorities of the service.

- e) Use the `S90sccd` and `K10sccd` links to test starting and stopping the service. The links are called automatically when the machine is started or shut down.

Configuring Memory Usage

(Optional) Determine whether you need to configure how much memory Sybase Control Center uses, and if so which configuration method to use.

It is not usually necessary to configure memory usage for Sybase Control Center. This table lists memory options you can set and circumstances under which you should consider changing them.

Modify this value	When	Guidelines
<p>Maximum memory</p> <ul style="list-style-type: none"> <code>jvmopt=-Xmx</code> – if you are running Sybase Control Center as a Windows service <code>SCC_MEM_MAX</code> – if you are running SCC as a UNIX service <code>SCC_MEM_MAX</code> – if you are starting SCC from the command line 	<ul style="list-style-type: none"> You need to prevent Sybase Control Center from using more than a given amount of memory Sybase Control Center fails to start and may display an error: <code>Could not create the Java Virtual machine.</code> An <code>OutOfMemory</code> error says Sybase Control Center is out of heap space A warning message about system memory appears during the start process The machine where Sybase Control Center is installed has less than 4GB of memory. (Starting Sybase Control Center on a machine with less than 4GB of memory triggers the startup warning message about system memory.) 	<p>On machines with less than 4GB of memory, set maximum memory to 256MB or more.</p> <p>Default value: none. (On machines with 4GB or more of memory, maximum memory is set dynamically and is effectively limited only by the amount of system memory available.)</p>

Modify this value	When	Guidelines
Permanent memory <ul style="list-style-type: none"> • <code>jvmopt=-XX:MaxPermSize</code> – if you are running Sybase Control Center as a Windows service • <code>SCC_MEM_PERM</code> – if you are running SCC as a UNIX service • <code>SCC_MEM_PERM</code> – if you are starting SCC from the command line 	An OutOfMemory error says Sybase Control Center is out of permanent generation space	Increase by 32MB increments. If you reach a value equal to twice the default and still see the OutOfMemory error, contact Sybase technical support. Default value: 128MB

You can change memory options in two ways:

- For Sybase Control Center started from the command line – execute commands to set one or more environment variables before executing the **scc** command to start Sybase Control Center. When you use this method, your changes to the memory options last only as long as the current login session. This method is useful for testing new option values.
- For the Sybase Control Center service – modify a file used by the Sybase Control Center service. When you use this method, your changes to the memory options persist—Sybase Control Center uses them every time it starts as a service.

See also

- *Logging in to Sybase Control Center* on page 46

Changing a Memory Option on the Command Line

Before you start Sybase Control Center from the command line, you can issue a command to change the value of a memory option temporarily.

Changes made using this method last only as long as the current login session. This method is useful for testing new option values.

1. If Sybase Control Center is running, shut it down.
2. Set the environment variable. Specify a size in megabytes but do not indicate the units in the command.

Windows example:

```
> set SCC_MEM_MAX=512
```

UNIX example:

```
bash$ export SCC_MEM_MAX=512
```

3. Use the **scc** command to start Sybase Control Center.

See also

- *Changing a Memory Option for a Sybase Control Center Windows Service* on page 45
- *Changing a Memory Option for an SCC UNIX Service* on page 45

Changing a Memory Option for a Sybase Control Center Windows Service

Add a **jvmopt** command to the `scc.properties` file to change a memory option (`-Xmx` or `-XX:MaxPermSize`) for a Sybase Control Center Windows service.

When you use this method to set memory options, your changes are permanent—Sybase Control Center uses them every time it starts as a service.

1. If Sybase Control Center is running, shut it down.
2. Open the Sybase Control Center properties file:

```
<Sybase Control Center-install-directory>\SCC-3_2\bin  
\scc.properties
```
3. Add (or modify, if it already exists) a **jvmopt** line specifying the memory size in Java format. Use `m` for megabytes or `g` for gigabytes.

For example:

```
jvmopt=-Xmx512m
```

4. Save the file and start the Sybase Control Center Windows service.

See also

- *Changing a Memory Option on the Command Line* on page 44
- *Changing a Memory Option for an SCC UNIX Service* on page 45

Changing a Memory Option for an SCC UNIX Service

To change a memory setting for a Sybase Control Center UNIX service, add the appropriate environment variable (`SCC_MEM_MAX` or `SCC_MEM_PERM`) to the `sccd` script.

When you use this method to set memory options, your changes are permanent—Sybase Control Center uses them every time it starts as a service.

1. If Sybase Control Center is running, shut it down.
2. Open the `sccd` file: `/etc/init.d/sccd`
3. Add the environment variable at the top of the file (after the comments). Specify a size in megabytes but do not indicate the units in the command.

For example:

```
SCC_MEM_MAX=512
```

Get Started

4. Save the file and start the Sybase Control Center UNIX service.

See also

- *Changing a Memory Option on the Command Line* on page 44
- *Changing a Memory Option for a Sybase Control Center Windows Service* on page 45

Logging in to Sybase Control Center

Enter the Sybase Control Center Web console.

Prerequisites

Install Adobe Flash Player in the browser you will use for SCC. See the *Sybase Control Center Installation Guide*.

Task

Sybase Control Center typically authenticates users through the operating system or an LDAP directory service. Consult your SCC administrator if you are not sure which login account to use for SCC.

Only one login session per account is permitted at a time; multiple users cannot be logged in to the same account simultaneously.

Note: When logging in to a newly installed Sybase Control Center for which secure authentication has not been configured, use the sccadmin account—the password is set during installation. For more information, see the *Sybase Control Center Installation Guide*.

1. Connect to the Sybase Control Center server. In your Web browser, enter: `https://scc-hostname:8283/scc`.
2. Enter your user name and password, and click **Login**.

Tip: If you use a Windows account to log in to SCC, enter your user name in the format `username@domain`. Omit top-level domain extensions such as `.com` or `.net`—for example, enter `fred@sap`, not `fred@sap.com`.

See also

- *Configuring Memory Usage* on page 43

Setting Up Security

Configure login authentication and map roles.

Read about security and follow these procedures before you configure Sybase Control Center product modules.

Note: These security topics are intended for use in a production environment. If you are evaluating or testing SCC, see *Quick Start for an Evaluation* on page 17.

1. *Security*

Sybase Control Center can authenticate user logins through an LDAP server, through the operating system, or both.

2. *Configuring Authentication for Windows*

Authentication through the Windows operating system is enabled by default. Configuration is required only if you have upgraded from an older version of Sybase Control Center and no longer want to use the older version's authentication settings; if you do not want to use Windows for authentication; or if you want to create login accounts manually. Sybase recommends that you allow SCC to create accounts automatically.

3. *Configuring a Pluggable Authentication Module (PAM) for UNIX*

Set up Sybase Control Center to support username and password login using accounts on the UNIX operating system.

4. *Configuring an LDAP Authentication Module*

Configure an LDAP authentication module for Sybase Control Center by editing the security configuration file to point to the correct LDAP server.

5. *Mapping Sybase Control Center Roles to LDAP or OS Groups*

To grant Sybase Control Center privileges to users who are authenticated through LDAP or the operating system, associate roles used in Sybase Control Center with groups in LDAP or the operating system.

6. *Encrypting a Password*

Use the `passencrypt` utility to encrypt passwords and other values that must be kept secure while stored in text files.

7. *Configuring Ports*

(Optional) Use the `scc --port` command to assign Sybase Control Center services to new ports.

See also

- *Configuring the E-mail Server* on page 66

Security

Sybase Control Center can authenticate user logins through an LDAP server, through the operating system, or both.

- Sybase Control Center can be configured to authenticate through any LDAP server that supports the `inetOrgPerson` (RFC 2798) schema.
- When Sybase Control Center authenticates through the operating system, it uses the operating system of the Sybase Control Center server machine (not the client).

Although you can create native user accounts in Sybase Control Center, Sybase does not recommend this approach to authentication. It is simpler and safer to configure Sybase Control Center to authenticate using existing LDAP, Windows, or UNIX login accounts.

Sybase strongly recommends that you use a common authentication provider for all Sybase products, including Sybase Control Center. A common authentication provider ensures that single sign-on works for users of Sybase Control Center and its managed servers.

Sybase Control Center requires each authenticated login account to have a predefined role. When a login is authenticated, roles for the login are retrieved by the security module and are mapped to Sybase Control Center predefined roles. Authorization is resolved through the mappings between the security module native roles and Sybase Control Center roles. You can enable mappings by creating a “sybase” group in your operating system or LDAP server and adding all Sybase Control Center users, or by modifying the Sybase Control Center `role-mapping.xml` file to configure the mapping of native roles to Sybase Control Center roles. The security module authenticates the logins and authorizes access to managed resources.

Sybase Control Center provides a set of predefined login modules for authentication. All login modules are defined in the `<install_location>/SCC-3_2/conf/csi_config.xml` file. The syntax is defined by the Sybase Common Security Infrastructure (CSI) framework. You can configure the different login modules to customize security strength. The login modules are:

- **Preconfigured user login** – defines a user name, password, and a list of roles. The default user name is `sccadmin`; its password is configured during installation and its native role is SCC Administrator, which maps to `sccAdminRole`. You can create additional accounts by adding preconfigured user login modules to `csi_config.xml`. However, Sybase does not recommend the use of preconfigured user login modules for authentication in production environments.
- **NT proxy login** – delegates authentication to the underlying Windows operating system. When you log in to Sybase Control Center through an NT Proxy Login module, enter your user name in the format `username@nt-domain-name`. For example, `user@sybase`. Windows authentication is enabled by default, but it requires some configuration after an upgrade from SCC 3.2.5 or earlier.
- **UNIX proxy login** – delegates authentication to the underlying UNIX or Linux operating system using Pluggable Authentication Modules (PAM). When you log in to Sybase Control Center through a UNIX PAM, enter your UNIX user name and password. UNIX authentication is enabled by default, but it requires some configuration.
- **LDAP login** – delegates authentication to an LDAP server you specify. When you log in to Sybase Control Center through an LDAP server, enter your LDAP user name and password. LDAP authentication is not enabled by default; you must configure the login module.

Configuring Authentication for Windows

Authentication through the Windows operating system is enabled by default. Configuration is required only if you have upgraded from an older version of Sybase Control Center and no longer want to use the older version’s authentication settings; if you do not want to use Windows for authentication; or if you want to create login accounts manually. Sybase recommends that you allow SCC to create accounts automatically.

This task is optional. However, if you choose not to create Sybase Control Center accounts automatically, you must enter them manually. Even when SCC users authenticate through LDAP or the local operating system, SCC needs the accounts for purposes of setting authorization (user privileges).

1. Log in to Sybase Control Center using an account with administrative privileges. (The login account or its group must have `sccAdminRole`.)
2. Select **Application > Administration > Security**.
3. Click to select or deselect the box labeled **Automatically add SCC login records for authenticated logins**.
4. Click to select or deselect the box labeled **Automatically grant sccUserRole to newly created logins**.
5. Click **OK** to close the Security dialog.

Next

There are two next steps:

- If you opted not to automatically create Sybase Control Center login accounts, enter each account into Sybase Control Center manually.
- Grant privileges to login accounts that require more than basic user access. You can grant privileges by assigning Sybase Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping Sybase Control Center roles to the groups. The group approach is generally more efficient.

Configuring a Pluggable Authentication Module (PAM) for UNIX

Set up Sybase Control Center to support username and password login using accounts on the UNIX operating system.

1. Using a login account with root privileges, configure the pluggable authentication module for your platform:

Platform	Action
Solaris	Append the contents of the <code><SCC-install-dir>/utility/<sunos>/pam.conf</code> file (provided with Sybase Control Center) to the <code>/etc/pam.conf</code> file on your Solaris platform.
Linux	<p>Copy the <code><SCC-install-dir>/utility/<linux>/sybase-csi</code> file (provided with Sybase Control Center) to the <code>/etc/pam.d</code> directory on your Linux platform.</p> <p>Note: The <code>sybase-csi</code> file provided with Sybase Control Center is not compatible with the most recent SUSE Linux versions. For SUSE 11 and later, see the example at the end of this topic.</p>

Note: In the table above, the portion of the path that indicates the operating system might differ slightly from what is shown.

2. If the host UNIX system is not using a directory lookup for authentication (yp or NIS, for example) and authentication is carried out against the local `/etc/passwd` file, change the permissions on `/etc/shadow` to provide read access to the login account that executes SCC.
3. (Skip if you configured a PAM before starting Sybase Control Center) Restart Sybase Control Center.
4. (Optional) Change account creation options.
 - a) Log in to Sybase Control Center using an account with administrative privileges (`sccAdminRole`).
 - b) Select **Application > Administration > Security**.
 - c) Click to select or deselect the box labeled **Automatically add SCC login records for authenticated logins**. (By default, this option is enabled for SCC 3.2.6 and later.)
 - d) Click to select or deselect the box labeled **Automatically grant sccUserRole to newly created logins**. (By default, this option is enabled for SCC 3.2.6 and later.)
 - e) Click **OK** to close the Security dialog.

Example: PAM for SUSE Linux 11 and later

For SUSE 11 and later, do not use the `sybase-csi` file provided with Sybase Control Center. Instead, in your `/etc/pam.d` directory, create a `sybase-csi` file that contains:

```
# sybase-csi PAM Configuration (SUSE style)
auth      include      common-auth
account   include      common-account
password  include      common-password
session   include      common-session
```

Next

There are two next steps:

- If you opted not to automatically create Sybase Control Center login accounts, enter each account into Sybase Control Center manually. Sybase Control Center needs the accounts for purposes of setting authorization (user privileges).
- Grant privileges to login accounts that require more than basic user access. You can grant privileges by assigning Sybase Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping Sybase Control Center roles to the groups. The group approach is generally more efficient.

See also

- *Mapping Sybase Control Center Roles to LDAP or OS Groups* on page 111
- *Adding a Login Account to the System* on page 123

Configuring an LDAP Authentication Module

Configure an LDAP authentication module for Sybase Control Center by editing the security configuration file to point to the correct LDAP server.

1. Open the <SCC-install-dir>\conf\csi_config.xml file.
2. Uncomment the LDAP module in the configuration file by removing the surrounding <!-- and --> characters (or, if necessary, add an LDAP module to the file). The sample module below specifies the LDAP server that will provide user authentication.

The sample module shows the properties used for an OpenDS LDAP server. See the example at the end of this task for values that work for ActiveDirectory. Configuration properties you can use in the LDAP module are described in a subtopic.

```
<authenticationProvider controlFlag="sufficient"
name="com.sybase.security.ldap.LDAPLoginModule">
  <options name="BindDN" value="cn=Directory Manager"/>
  <options name="BindPassword" value="secret"/>
  <options name="DefaultSearchBase" value="dc=example,dc=com"/>
  <options name="ProviderURL" value="ldap://localhost:10389"/>
  <options name="ServerType" value="openldap"/>
</authenticationProvider>
<provider name="com.sybase.security.ldap.LDAPAttributer"
type="attributer"/>
```

Note: Change only values shown in bold. If BindPassword is encrypted (which Sybase recommends), the line that defines it must include encrypted="true". The line should look similar to this:

```
<options name="BindPassword" encrypted="true"
value="lsnjikfwregfqr43hu5io..."/>
```

3. Save the file.
4. If your LDAP server's SSL certificate is signed by a nonstandard certificate authority (for example, if it is a self-signed certificate), use the **keytool** utility to configure your JVM or JDK to trust the certificate. Execute a command similar to this:

Windows:

```
keytool -import -keystore %SYBASE_JRE7%\lib\security\cacerts -
file <your cert file and path>
-alias ldapcert -storepass changeit
```

UNIX:

```
keytool -import -keystore $SYBASE_JRE7/lib/security/cacerts -file
<your cert file and path>
-alias ldapcert -storepass changeit
```

LDAP Configuration Values for ActiveDirectory

For an ActiveDirectory server, use these values for configuration properties in your LDAP login module:

```
ServerType: msad2K
DefaultSearchBase: dc=<domainname>,dc=<tld> or o=<company
name>,c=<country code>
                  E.g. dc=sybase,dc=com or o=Sybase,c=us
ProviderUrl: ldaps://<hostname>:<port>
                  E.g.: ldaps://myserver:636
AuthenticationFilter: (&(userPrincipalName={uid})
(objectclass=user))
BindDN: <User with read capability for all users>
BindPassword: <Password for BindDN user>
RoleFilter: (|(objectclass=groupofnames) (objectclass=group))
controlFlag: sufficient
```

Next

Map Sybase Control Center roles to LDAP groups.

See also

- *Mapping Sybase Control Center Roles to LDAP or OS Groups* on page 61

LDAP Configuration Properties

Use these properties in your `csi_config.xml` file to control the Sybase Control Center LDAP service.

Note: These characters have special meaning when they appear in a name in LDAP: , (comma), = (equals), + (plus), < (less than), > (greater than), # (number or hash sign), ; (semicolon), \ (backslash), / (forward slash), LF (line feed), CR (carriage return), " (double quotation mark), ' (single quotation mark), * (asterisk), ? (question mark), & (ampersand), and a space at the beginning or end of a string. LDAP providers do not handle these special characters in any of the names or DN's in any of the configuration properties. Additionally, some of the properties, as identified below, cannot use these special characters in common names.

Property	Default Value	Description
ServerType	None	<p>Optional. The type of LDAP server you are connecting to:</p> <ul style="list-style-type: none"> • sunone5 -- SunOne 5.x OR iPlanet 5.x • msad2k -- Microsoft Active Directory, Windows 2000 • nsds4 -- Netscape Directory Server 4.x • openldap -- OpenLDAP Directory Server 2.x <p>The value you choose establishes default values for these other authentication properties:</p> <ul style="list-style-type: none"> • RoleFilter • UserRoleMembership • RoleMemberAttributes • AuthenticationFilter • DigestMD5Authentication • UseUserAccountControl
ProviderURL	ldap://local-host:389	<p>The URL used to connect to the LDAP server. Use the default value if the server is:</p> <ul style="list-style-type: none"> • Located on the same machine as your product that is enabled with the common security infrastructure. • Configured to use the default port (389). <p>Otherwise, use this syntax for setting the value:</p> <p>ldap://<hostname>:<port></p>

Property	Default Value	Description
DefaultSearchBase	None	<p>The LDAP search base that is used if no other search base is specified for authentication, roles, attribution, and self registration:</p> <ol style="list-style-type: none"> 1. <code>dc=<domainname>,dc=<tld></code> For example, a machine in the sybase.com domain would have a search base of <code>dc=sybase,dc=com</code>. 2. <code>o=<company name>,c=<country code></code> For example, this might be <code>o=Sybase,c=us</code> for a machine within the Sybase organization. <hr/> <p>Note: When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> • Do not use special characters, as listed above, in common names or distinguished names in the value of this property. • Do not use Chinese or Japanese characters in user names or passwords of this property.
SecurityProtocol	None	<p>The protocol to be used when connecting to the LDAP server.</p> <p>To use an encrypted protocol, use <code>ssl</code> instead of <code>ldaps</code> in the URL.</p>
AuthenticationMethod	Simple	<p>The authentication method to use for all authentication requests into LDAP. Legal values are generally the same as those of the <code>java.naming.security.authentication</code> JNDI property. Choose one of:</p> <ul style="list-style-type: none"> • <code>simple</code> — For clear-text password authentication. • <code>DIGEST-MD5</code> — For more secure hashed password authentication. This method requires that the server use plain text password storage and only works with JRE 1.4 or later.

Property	Default Value	Description
AuthenticationFilter	<p>For most LDAP servers: (&uid={uid})(objectclass=person))</p> <p>or</p> <p>For Active Directory e-mail lookups: (&userPrincipalName={uid})(objectclass=user)[ActiveDirectory]</p> <p>For Active Directory Windows user name lookups: (&sAMAccountName={uid})(objectclass=user)</p>	<p>The filter to use when looking up the user.</p> <p>When performing a user name based lookup, this filter is used to determine the LDAP entry that matches the supplied user name.</p> <p>The string "{uid}" in the filter is replaced with the supplied user name.</p> <hr/> <p>Note: When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> Do not use special characters, as listed above, in common names or distinguished names in the value of this property. Do not use Chinese or Japanese characters in user names or passwords of this property. <hr/>
AuthenticationScope	onelevel	<p>The authentication search scope. The supported values for this are:</p> <ul style="list-style-type: none"> onelevel subtree <p>If you do not specify a value or if you specify an invalid value, the default value is used.</p>

Property	Default Value	Description
AuthenticationSearchBase	None	<p>The search base used to authenticate users. If this property is not configured, the value for DefaultSearchBase is used.</p> <hr/> <p>Note: When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> • Do not use special characters, as listed above, in common names or distinguished names in the value of this property. • Do not use Chinese or Japanese characters in user names or passwords of this property. <hr/>
BindDN	None	<p>The user DN to bind against when building the initial LDAP connection.</p> <p>In many cases, this user may need read permissions on all user records. If you do not set a value, anonymous binding is used. Anonymous binding works on most servers without additional configuration.</p> <p>However, the LDAP attributer may use this DN to create users in the LDAP server. When the self-registration feature is used, this user may need permissions to create a user record. This behavior may occur if you do not set useUserCredentialsToBind to true. In this case, the LDAP attributer uses this DN to update the user attributes.</p>

Property	Default Value	Description
BindPassword	None	<p>The password for BindDN, which is used to authenticate any user. BindDN and BindPassword separate the LDAP connection into units.</p> <p>The AuthenticationMethod property determines the bind method used for this initial connection.</p> <p>Sybase recommends that you encrypt passwords, and provides a password encryption utility. If you encrypt BindPassword, include <code>encrypted=true</code> in the line that sets the option. For example:</p> <pre><options name="BindPassword" encrypted="true" value="lsnjikf-wregfqr43hu5io..." /></pre> <p>If you do not encrypt BindPassword, the option might look like this:</p> <pre><options name="BindPassword" value="s3cr3T" /></pre>
RoleSearchBase	None	<p>The search base used to retrieve lists of roles. If this property is not configured, LDAP uses the value for DefaultSearchBase.</p> <hr/> <p>Note: When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> Do not use special characters, as listed above, in common names or distinguished names in the value of this property. Do not use Chinese or Japanese characters in user names or passwords of this property. <hr/>

Property	Default Value	Description
RoleFilter	<p>For SunONE/iPlanet: (<code>&</code>; (object-class=ldapsubentry) (object-class=nsroledefinition))</p> <p>For Netscape Directory Server: (<code> </code> (object-class=groupofnames) (object-class=groupofuniquenames))</p> <p>For ActiveDirectory: (<code> </code> (object-class=groupofnames) (object-class=group))</p>	<p>The role search filter. This filter should, when combined with the role search base and role scope, return a complete list of roles within the LDAP server. There are several default values, depending on the chosen server type. If the server type is not chosen and this property is not initialized, no roles are available.</p> <hr/> <p>Note: When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> Do not use special characters, as listed above, in common names or distinguished names in the value of this property. Do not use Chinese or Japanese characters in user names or passwords of this property. <hr/>
RoleMemberAttributes	For Netscape Directory Server and OpenLDAP Server: member,unique-member	<p>A comma-separated list of role attributes from which LDAP derives the DN's of users who have this role.</p> <p>These values are cross-referenced with the active user to determine the user's role list. One example of the use of this property is when using LDAP groups as placeholders for roles. This property has a default value only when the Netscape server type is chosen.</p>
RoleNameAttribute	cn	The attribute of the role entry used as the role name. This is the role name displayed in the role list or granted to the authenticated user.
RoleScope	onelevel	<p>The role search scope. Supported values include:</p> <ul style="list-style-type: none"> onelevel subtree <p>If you do not specify a value or if you specify an invalid value, LDAP uses the default value.</p>

Property	Default Value	Description
SkipRoleLookup	false	<p>Set this property to true to grant the roles looked up using the attributes specified by the property UserRoleMembershipAttributes without cross-referencing them with the roles looked up using the RoleSearchBase and RoleFilter.</p> <p>LDAP configuration validation succeeds even when an error is encountered when listing all the available roles. The error is logged to the server log during validation but not reported in SCC, allowing the configuration to be saved. This has an impact when listing the physical roles for role mapping as well as in SCC. To successfully authenticate the user, set the SkipRoleLookup property to true.</p>
UserRoleMembershipAttributes	<p>For iPlanet/SunONE: nsRoleDN</p> <p>For Active Directory: memberOf</p> <p>For all others: none</p>	<p>Defines a user attribute that contains the DNs of all of the roles a user is a member of.</p> <p>These comma-delimited values are cross-referenced with the roles retrieved in the role search base and search filter to generate a list of user's roles.</p> <p>If the SkipRoleSearch property is set to true, these comma-delimited values are not cross-referenced with the roles retrieved in the role search base and role search filter. See <i>SkipRoleLookup</i>.</p> <hr/> <p>Note: If you use nested groups with Active Directory, you must set this property to tokenGroups.</p>
UserFreeformRoleMembershipAttributes	None	<p>The free-form role membership attribute list. Users who have attributes in this comma-delimited list are automatically granted access to roles whose names are equal to the attribute value. For example, if the value of this property is department and the department attribute in the user's LDAP record has the values {sales, consulting}, the user is granted the roles sales and consulting.</p>
Referral	ignore	<p>The behavior when a referral is encountered. Valid values are dictated by LdapContext, but might include follow, ignore, or throw.</p>

Property	Default Value	Description
DigestMD5Authentication-Format	DN For OpenLDAP: User name	The DIGEST-MD5 bind authentication identity format.
UseUserAccountControlAttribute	For Active Directory: true	When this property is set to true, the UserAccountControl attribute detects disabled user accounts, account expirations, password expirations, and so on. Active Directory also uses this attribute to store the above information.
EnableLDAPConnectionTrace	False	Enables LDAP connection tracing. The output is logged to a file in the temp directory. The location of the file is logged to the server log.
ConnectTimeout	0	Specifies the timeout, in milliseconds, for attempts to connect to the LDAP server. The property value sets the JNDI com.sun.jndi.ldap.connect.timeout property when attempting to establish a connection to a configured LDAP server. If the LDAP provider cannot establish a connection within the configured interval, it aborts the connection attempt. An integer value less than or equal to zero results in the use of the network protocol's timeout value.
ReadTimeout	0	Controls the length of time, in milliseconds, the client waits for the server to respond to a read attempt after the initial connection to the server has been established. The property values sets the JNDI com.sun.jndi.ldap.read.timeout property when attempting to establish a connection to a configured LDAP server. If the LDAP provider does not receive an LDAP response within the configured interval, it aborts the read attempt. The read timeout applies to the LDAP response from the server after the initial connection is established with the server. An integer value less than or equal to zero indicates no read timeout is specified.

Property	Default Value	Description
LDAPPoolMaxActive	8	Caps the number of concurrent LDAP connections to the LDAP server. A non-positive value indicates no limit. If this option is set for multiple LDAP providers, the value set by the first LDAP provider loaded takes precedence over all the others. When LDAPPoolMaxActive is reached, any further attempts by the LDAP provider classes to borrow LDAP connections from the pool are blocked indefinitely until a new or idle object becomes available in the pool. Connection pooling improves the LDAP provider's performance and resource utilization by managing the number of TCP connections established with configured LDAP servers.
controlFlag	optional	When you configure multiple authentication providers, use controlFlag for each provider to control how the authentication providers are used in the login sequence. controlFlag is a generic login module option rather than an LDAP configuration property.

Mapping Sybase Control Center Roles to LDAP or OS Groups

To grant Sybase Control Center privileges to users who are authenticated through LDAP or the operating system, associate roles used in Sybase Control Center with groups in LDAP or the operating system.

Prerequisites

- Required: Configure an LDAP authentication module.
- Optional: Create these LDAP groups and assign Sybase Control Center users to them:
 - sybase – confers sccUserRole. Assign all SCC users to the sybase group.
 - SCC Administrator – confers sccAdminRole. Assign only SCC administrators to this group.

Task

You can configure Sybase Control Center to enable users to authenticate through their local operating system or through an LDAP server. To make this type of authentication work, SCC roles must be mapped to groups that exist in the system providing authentication (LDAP or the operating system).

The sybase and SCC Administrator groups are convenient because they are predefined in `role-mapping.xml`. If you add sybase and SCC Administrator groups to your LDAP

Get Started

system and populate them with SCC users and administrators, you can skip to the next task—you do not need to complete the steps below.

The table lists default mappings of LDAP and OS groups to SCC roles. Login modules are defined in `csi_config.xml`.

Login Module	OS Group	Sybase Control Center Roles
UNIX Proxy	root	uaAnonymous, uaAgentAdmin, uaOSAdmin
	sybase	uaAnonymous, uaPluginAdmin, sccUserRole
	user	uaAnonymous
	guest	uaAnonymous
NT Proxy	Administrators	uaAnonymous, uaAgentAdmin, uaOSAdmin
	sybase	uaAnonymous, uaPluginAdmin, sccUserRole
	Users	uaAnonymous
	Guests	uaAnonymous
LDAP	sybase	uaAnonymous, uaPluginAdmin, sccUserRole
	SCC Administrator	uaAnonymous, sccAdminRole

There are two ways to accomplish the mapping:

- (Recommended) Add a “sybase” group and an “SCC Administrator” group to the operating system or LDAP server Sybase Control Center is using to authenticate users, and add all users who need to access Sybase Control Center to one or both groups.
- Configure Sybase Control Center to use existing groups in LDAP or the operating system by editing the `role-mapping.xml` file. This option is described here.

1. If Sybase Control Center is running, shut it down.

2. In a text editor, open:

```
<SCC-install-directory>/conf/role-mapping.xml
```

3. Locate the `sccUserRole` section of the file:

```
<Mapping>
  <LogicalName>sccUserRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
  <MappedName>SCC Agent Administrator</MappedName>
  <MappedName>sybase</MappedName>
</Mapping>
```

4. Add a `MappedName` line for the LDAP or OS group you are using to authenticate SCC users. The `sccUserRole` section should look similar to this:

```
<Mapping>
  <LogicalName>sccUserRole</LogicalName>
```

```

    <MappedName>SCC Administrator</MappedName>
    <MappedName>SCC Agent Administrator</MappedName>
    <MappedName>sybase</MappedName>
    <MappedName>my_SCC_group</MappedName>
  </Mapping>

```

5. Locate the sccAdminRole section of the file:

```

<Mapping>
  <LogicalName>sccAdminRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
</Mapping>

```

6. Add a MappedName line for the LDAP or OS group you are using to authenticate SCC administrators. The sccAdminRole section should look similar to this:

```

<Mapping>
  <LogicalName>sccAdminRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
  <MappedName>my_SCC_admin_group</MappedName>
</Mapping>

```

7. Save the file and exit.
8. (LDAP only) Ensure that the roles defined in the LDAP repository match the roles defined in role-mapping.xml.
9. In the <SCC-install-dir>\conf\csi_config.xml file, set the BindPassword and ProviderURL properties with values used in your deployment.
Sybase recommends that you encrypt sensitive values before saving them in csi_config.xml.
10. Start Sybase Control Center.

See also

- *Configuring an LDAP Authentication Module* on page 51

Encrypting a Password

Use the **passencrypt** utility to encrypt passwords and other values that must be kept secure while stored in text files.

You can safely store an encrypted password in a configuration file. Enter the password in clear text (unencrypted) when you execute **passencrypt** and when you use the password to log in.

passencrypt, which is located in the Sybase Control Center bin directory, uses the SHA-256 hash algorithm for passwords used in the PreConfiguredLoginModule in csi_config.xml.

1. Open a command window and change to the bin directory:

Windows: cd <SCC-install-directory>\bin

UNIX: cd <SCC-install-directory>/bin

2. To encrypt a password, enter **passencrypt -csi**. Enter your new password at the resulting prompt.

passencrypt encrypts the password you enter (which does not appear on the screen) and displays the password in encrypted form.

3. Copy the encrypted password.
4. Paste the encrypted password where needed.

Configuring Ports

(Optional) Use the **scc --port** command to assign Sybase Control Center services to new ports.

Prerequisites

Check for port conflicts between Sybase Control Center and other software running on the same host.

Task

Sybase Control Center cannot function properly if other services use its ports. If you discover a conflict with any port listed in the right column below, you can either reconfigure the other service's port or reconfigure Sybase Control Center as described here.

Port Name	Description	Service Names	Property Names	Default Port
db	Database port Present on SCC server	SccSADataserver Messaging Alert Scheduler	com.sybase.asa.server.port messaging.db.port alert.database.port org.quartz.data-Source.ASA.URL	3638
http	Web HTTP port Present on SCC server	EmbeddedWebCon- tainer	http.port	8282
https	Web HTTPS (secure HTTP) port Present on SCC server	EmbeddedWebCon- tainer	https.port	8283
jiniHttp	JINI HTTP server Present on SCC server and SCC agent	Jini	httpPort	9092

Port Name	Description	Service Names	Property Names	Default Port
jiniR-mid	JINI remote method invocation daemon Present on SCC server and SCC agent	Jini	rmiPort	9095
msg	Messaging port Present on SCC server	Messaging	messaging.port	2000
rmi	RMI port Present on SCC server and SCC agent	RMI	port	9999
tds	Tabular Data Stream™ port (used to communicate with other Sybase products) Present on SCC server and SCC agent	Tds	tdsPort	9998

1. Shut down Sybase Control Center.
2. Execute **scc --info ports** to display a list of Sybase Control Center services, their properties, and their assigned ports.
3. To reassign a port, enter a command in one of these formats:
`scc --port port-name=port-number`
`scc --port service-name:property-name=port-number`

Use the first, simpler format unless you want to configure the database services to use different ports. (By default, they all use the same port.)

4. Start Sybase Control Center.
5. Execute **scc --info ports** again to confirm that the port has been reassigned.

Examples

Set all four database services (data server, messaging, database alert, and scheduler) to the same port, 3639. (The database is SQL Anywhere®, used by the Sybase Control Center internal repository.)

```
scc --port db=3639
```

Set only the database messaging service to port 3639.

```
scc --port Messaging:messaging.db.port=3639
```

Set the HTTP port to 9292.

Get Started

```
scc --port http=9292
```

Set the Jini RMI daemon to port 9696.

```
scc --port jiniRmid=9696
```

Set the main Sybase Control Center messaging service to port 2001.

```
scc --port msg=2001
```

Set the RMI port to 9991.

```
scc --port rmi=9991
```

Set the Tabular Data Stream port to 9997.

```
scc --port tds=9997
```

Note: **scc** commands that include a port-setting option (**-p** or **--port**) do not start Sybase Control Center. To start SCC, execute a separate **scc** command.

Configuring the E-mail Server

(Optional) Specify the e-mail server for Sybase Control Center to use to send e-mail alert notifications.

Prerequisites

Launch Sybase Control Center and log in using an account with administrative privileges. (The login account or its group must have sccAdminRole.)

Task

1. From the application's menu bar, select **Application > Administration**.
2. Select **General Settings**.
3. Click the **E-mail** tab.
4. Enter the name of the e-mail server through which Sybase Control Center will send alert notifications.
5. Change the default e-mail server port only in consultation with your e-mail administrator.
6. (Optional) Click **Customize e-mail settings** to display options for setting the domain name and e-mail sender for alert e-mail notifications.
7. (Optional) Enter your domain name (for example, mycompany.com).

Most e-mail servers do not require SCC to provide an explicit domain name. Try providing a domain name here if your first attempt to configure e-mail alerts fails.

8. (Optional) Change the default e-mail sender name.

This name appears in the "From" field of SCC e-mail alert messages. Do not use spaces; use hyphens or underscore characters instead.

Tip: If you have multiple SCC servers, configure their sender names so you can tell which SCC an alert is coming from. For example, SybaseControlCenter_Boston or SCC_test11.

9. (Optional) If you entered anything in the **E-mail Domain name** or **E-mail sender name** fields, click **Apply** to make the test e-mail option reappear.
10. (Optional) To dispatch a test message, enter an e-mail address in the **Test e-mail address** field and click **Send**.
If the test e-mail is received, you have properly configured the server for e-mail alert notifications.
11. Click **OK** (to apply the change and close the properties dialog) or **Apply** (to apply the change and leave the dialog open).

Next

(Optional) Configure automatic logout.

See also

- *Setting Up Security* on page 46

Configuring the Automatic Logout Timer

(Optional) Set Sybase Control Center to end login sessions when users are inactive for too long.

Prerequisites

Launch Sybase Control Center and log in using an account with administrative privileges. (The login account or its group must have sccAdminRole.)

Task

1. From the application's menu bar, select **Application > Administration**.
2. Select **General Settings**.
3. Click the **Auto-Logout** tab.
4. Enter the number of minutes after which an idle user will be automatically logged out.
Enter 0 or leave the box empty to disable automatic logout.
5. Click **OK** (to apply the change and close the properties dialog) or **Apply** (to apply the change and leave the dialog open).

User Authorization

The authorization mechanism in Sybase Control Center employs login accounts and task-based roles.

Access to Sybase Control Center is controlled by login accounts. You grant permissions to a login account by assigning predefined roles that control tasks the user can perform in Sybase Control Center, such as administration and monitoring of particular types of Sybase servers.

The roles can be assigned directly to login accounts or to groups; a login account inherits the roles of any group to which it belongs. Component product modules assign some roles automatically.

Sybase Control Center classifies roles as follows:

- System roles – define how a user can interact with Sybase Control Center.
- Product roles – define how a user can interact with a particular managed resource in Sybase Control Center, for example the Replication Server named RepBoston01.

Note: The tools described here are for managing SCC-enabled login accounts; you cannot use them to manage accounts and groups that are native to your managed resource.

See also

- *Configure Sybase Control Center* on page 71

Assigning a Role to a Login or a Group

Use the security configuration options to add one or more roles to a Sybase Control Center login account or to a group. Roles enable users to perform tasks such as monitoring servers or administering Sybase Control Center.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task. To assign a monitoring role for a server, first register the server.

Task

Assign the sccAdminRole to any login account that will perform administrative tasks in Sybase Control Center.

1. From the application menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Click **Logins** or **Groups**.
4. In the table, select the login account or group to which you want to assign a role.
5. Click the **Roles** tab.
6. In the **Available roles for resource** list, select the role, then click **Add**. For example, to grant administrative privileges, add the SCC Service:sccAdminRole. To grant monitoring privileges, add the MonitorRole for the desired server and server type.

Note: Sybase Control Center product modules assign certain roles automatically, so you might not need to add a MonitorRole.

If a role appears in the **Has following roles** list, this account or group has already been configured with that role.

7. Click **OK**.

See also

- *Adding a Group* on page 69
- *Adding a Login Account to a Group* on page 69
- *Logins, Roles, and Groups* on page 70

Adding a Group

Use the security configuration options to create a new group.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

Groups can make roles easier to manage. Rather than assigning roles to individual users, assign roles to groups and add users to the groups or remove them as needed.

1. From the main menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Groups**.
4. Click **Create Group**.
5. Enter a group name and a description.
6. Click **Finish**.

See also

- *Assigning a Role to a Login or a Group* on page 68
- *Adding a Login Account to a Group* on page 69
- *Logins, Roles, and Groups* on page 70

Adding a Login Account to a Group

Use the security configuration options to add one or more login accounts to a group.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

1. From the main menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Click **Groups**.
4. Select the group to which you want to assign an account.
5. Click the **Membership** tab.

6. Select the account, then click **Add**.

7. Click **OK**.

See also

- *Assigning a Role to a Login or a Group* on page 68
- *Adding a Group* on page 69
- *Logins, Roles, and Groups* on page 70

Logins, Roles, and Groups

Sybase Control Center includes predefined login accounts and roles.

A login account identifies a user who can connect to Sybase Control Center. An account has roles that control the tasks the user is allowed to perform. Users can be authenticated through native SCC accounts, but a safer approach is to delegate authentication to the operating system or to an LDAP directory service.

Sybase Control Center comes with a predefined login account. Sybase recommends using the predefined account only for installing and setting up Sybase Control Center. This account is not intended for use in a production environment.

Table 10. Predefined Login Account

Login Name	Description
sccadmin	Can use all the administration features in Sybase Control Center. Use for configuration and test.

A role is a predefined profile that can be assigned to a login account or a group. Roles control the access rights for login accounts. Sybase Control Center comes with predefined roles that are intended for use in production environments.

Table 11. Predefined Roles

Role	Description
sccUserRole	Provides nonadministrative access to Sybase Control Center. Required for all users and assigned automatically to every authenticated user.
sccAdminRole	Provides administrative privileges for managing Sybase Control Center.

Monitoring privileges for SCC product modules are assigned automatically.

A group is made up of one or more login accounts; all the accounts in a group have the roles granted to the group. In Sybase Control Center you can create groups to suit your business requirements.

See also

- *Assigning a Role to a Login or a Group* on page 68
- *Adding a Group* on page 69
- *Adding a Login Account to a Group* on page 69

Configure Sybase Control Center

Configure Sybase Control Center for SAP Sybase IQ.

Note: Before configuring Sybase Control Center for use in a production environment, complete the tasks in the *Get Started* section of the help. Setting up security is particularly important.

1. *Configuring SAP Sybase IQ Authority-Based Users for Monitoring*

For 15.3 and 15.4 databases, enable one or more SAP Sybase IQ authority-based users to authenticate an SAP Sybase IQ server with Sybase Control Center, create and populate the SCC_MONITOR group.

2. *Configuring SAP Sybase IQ Roles-Based Users for Monitoring*

For 16.0 and later databases, enable one or more SAP Sybase IQ role-based users or roles to authenticate an SAP Sybase IQ server with Sybase Control Center, create and populate the SCC_MONITOR role.

3. *Registering an SAP Sybase IQ Server*

Make Sybase Control Center aware of an SAP Sybase IQ resource (for example, a server that can be monitored) and its connection information by registering the resource.

4. *Configuring SAP Sybase IQ for Administration*

To perform administration tasks, you must have the correct authority or group membership (15.3 or 15.4) or system privileges and role membership (16.0), and you may need to register the server's Sybase Control Center agent.

5. *Importing Resources for Batch Registration*

(Optional) Import and register multiple servers from an interfaces or sql.ini file.

6. *Registering and Authenticating a Sybase Control Center Agent*

Register and authenticate the Sybase Control Center agent for a managed server.

7. *Creating a Perspective*

Create a perspective in which you can add and manage resources.

8. *Adding a Resource to a Perspective*

Add one or more resources to the current perspective.

9. *Authenticating a Login Account for a Managed Resource*

Specify the login account and password Sybase Control Center will use when it connects to your server or agent to collect monitoring data or manage the resource.

10. *Changing Update Frequency for Statistics and Charts*

You can control the rate at which data on monitor screens and charts is refreshed, the amount of time covered by charts, and the multiplex nodes included in charts.

11. *Setting Up Statistics Collection*

Use the Properties view of your managed resource to create a data collection job and add a schedule to the job.

12. *Creating an Alert*

Use the Add Alert wizard to create an alert instance for your resource.

13. *Key Performance Indicators for SAP Sybase IQ*

Key performance indicators (KPIs) provide the statistics that appear on SAP Sybase IQ screens and charts in Sybase Control Center.

14. *Optional Configuration Steps*

Perform additional configuration, including user authorization, alerts, data collection scheduling, backups, and setting purging options for the repository.

See also

- *User Authorization* on page 67
- *Logins, Roles, and Groups* on page 125
- *Setting Up Security* on page 96
- *Assigning a Role to a Login or a Group* on page 119

Deploying an Instance from a Shared Disk Installation

(Optional) Create a Sybase Control Center server or agent from an installation on a shared disk.

Prerequisites

- Install Sybase Control Center on a shared disk.
- Enable shared-disk mode.

Task

1. Log in to the host on which you plan to run the SCC server or agent.

Note: You can create an instance on one host and run it on another host, but doing so interferes with the predeployment checks run by **sccinstance**. Such a deployment might generate errors (port conflicts, for example). If you are confident that the errors are caused by problems that will not be present on the host where you plan to run the instance, use the **-force** option to create the instance.

2. Change to `SCC-3_2/bin`.

3. Create the instance as an SCC agent if you plan to run a managed server on this host. Create the instance as an SCC server if you plan to manage other Sybase servers from this host.

To create an SCC agent called Boston-agent and configure it to run as a Windows service:

```
sccinstance -create -agent -instance Boston-agent -service
```

To create an SCC server called Boston and configure it to run as a Windows service:

```
sccinstance -create -server -instance Boston -service
```

On UNIX systems, omit the **-service** option.

4. If other SCC instances will run on this host, change the port assignments for the new instance. Change the instance names and port values in the sample commands to suit your environment, but take care to specify ports that are not in use by another SCC instance or any other application or server.

This command changes the port assignments for an SCC agent called myagent:

```
sccinstance -refresh -instance myagent -portconfig  
rmi=8888,jiniHttp=9093,jiniRmi=9096,tds=9997
```

This command changes the port assignments for an SCC server called myserver:

```
sccinstance -refresh -server -instance myserver -portconfig  
rmi=8889,db=3640,  
http=7072,https=7073,jiniHttp=9094,jiniRmi=9097,msg=2002,tds=9996
```

5. (Optional) List the instances deployed from this installation:

```
sccinstance -list
```

6. (Optional) If you are setting up an instance in UNIX, configure it to run as a service. See *Starting and Stopping Sybase Control Center in UNIX*.

Next

When you manage and maintain instances, keep in mind that the directory structure for instances is different from that of singleton installations. In file paths in SCC help, replace SCC-3_2 or <scc-install-directory> with SCC-3_2/instances/<instance-name>.

For example, the path to the log directory, SCC-3_2/log, becomes this for an instance called kalamazoo:

```
SCC-3_2/instances/kalamazoo/log
```

Enabling and Disabling Shared-Disk Mode

Turn on or turn off shared-disk mode, which allows you to run multiple Sybase Control Center agents and servers from a single installation on a shared disk.

Prerequisites

Install Sybase Control Center on a shared disk. See the *Sybase Control Center Installation Guide*.

Task

Shared-disk mode affects the entire installation; do not enable or disable individual instances.

Disabling shared-disk mode leaves the instances' file systems intact under <SCC-install-directory>/instances, but the instances cannot run. If you reenable, the instances are able to run again.

1. Change to SCC-3_2/bin.
2. Enable or disable shared disk mode.

To enable shared disk mode:

```
sccinstance -enable
```

To disable shared disk mode:

```
sccinstance -disable
```

See also

- *Shared-Disk Mode* on page 74
- *sccinstance Command* on page 75

Shared-Disk Mode

Shared-disk mode lets you run multiple Sybase Control Center instances—SCC servers, SCC agents, or a mixture of the two—from a single installation of the product.

The shared-disk capability enables SCC servers or agents on the installation host or on remote hosts to access and execute from the same installation. This feature is especially useful if you plan to use SCC to manage Adaptive Server® clusters, SAP Sybase ESP clusters, or SAP Sybase IQ multiplexes.

After installing SCC on a shared disk, use the **sccinstance** command to enable shared-disk mode and deploy instances. **sccinstance** copies the files needed for the instance into a new directory structure. The path takes the form <SCC-install-directory>/instances/<instance-name> (for example, SCC-3_2/instances/SCCserver-1).

You can specify a name for each instance. If you do not supply a name, the instance name defaults to the host name.

An instance runs on the host on which you start it. When shared-disk mode is enabled, SCC servers and agents run out of the `SCC-3_2/instances` subdirectories, not from the base file system.

In shared-disk mode, changes made to configuration files in the base file system (everything under `SCC-3_2` except the `SCC-3_2/instances` branch) are copied to any instance deployed thereafter. Previously deployed instances are not affected.

Use **sccinstance** to deploy, remove, refresh, or convert an instance; to configure an instance's ports; and to configure a Windows instance to run as a service. Perform other tasks, including configuring a UNIX instance to run as a service, and all other configuration, using the tools and procedures documented for all installations. Use tools provided by the UI wherever possible. When you must edit a file to change the configuration of an instance (for role mapping, for example), edit the copy of the file stored under `<SCC-install-directory>/instances/<instance-name>`.

See also

- *Enabling and Disabling Shared-Disk Mode* on page 74
- *sccinstance Command* on page 75

sccinstance Command

Use **sccinstance.bat** (Windows) or **sccinstance** (UNIX) to deploy an instance of Sybase Control Center from a shared-disk installation or to manage existing instances.

You can run multiple instances of Sybase Control Center, including SCC servers, SCC agents, or a mixture of the two, from a single installation on a shared disk.

Syntax

```
sccinstance[.bat]
[-agent]
[-c | -create]
[-d | -debug]
[-disable]
[-enable]
[-f | -force]
[-h | -help]
[-host host-name]
[-i | -instance [instance-name]]
[-l | -list]
[-plugins {plugin-ID,plugin-ID,...}]
[-portconfig {port-name=port-number,port-name=port-number, ...}]
[-refresh]
[-r | -remove]
[-s | -server]
[-service]
[-silent]
```

Parameters

- **-agent** – use with **-create** or **-refresh** to create or refresh an SCC agent. In a **-create** or **-refresh** command, **-agent** is the default, so you can omit it.
- **-create** – deploy a new instance. Use alone or with **-agent** to create an agent instance, or with **-server** to create a server instance.
- **-d | debug** – display debugging messages with the output of this command.
- **-disable** – turn off shared-disk mode for this installation. Generates an error if any instance is running.
- **-enable** – turn on shared-disk mode for this installation. Shared-disk mode is required if you intend to run more than one server or agent from a single installation of SCC.
- **-f | -force** – execute **sccinstance** even if there are potential conflicts, such as port clashes or a running SCC process. Sybase does not recommend using **-force** to remove or refresh a running instance in a Windows environment.
- **-h | --help** – display help and usage information for the **sccinstance** command.
- **-host *host-name*** – specify the host for this instance. Use with **-create**; required only when the instance name does not match the name of the host on which this instance will run. (The instance name defaults to the name of the current host unless you use **-instance** to specify another name.)
- **-instance [*instance-name*]** – specify an instance. Use with **-create**, **-remove**, or **-refresh**, or use alone to display the instance's status. You can omit **-instance** when you are addressing the only SCC instance or the only instance of the specified type (server or agent) on the current host.

sccinstance assumes that the host name is the same as the instance name unless you use **-host** to specify a different host name.

- **-l | -list** – display a list of all instances deployed from this SCC installation.
- **-plugins {*plugin-ID,plugin-ID,...*}** – specify one or more product module plug-ins for this instance. An alternative to **-agent** and **-server**, **-plugins** is primarily for use by the SCC installation program. Use with **-create** or **-refresh**. Use commas to separate plug-in names.
- **-portconfig {*port-name=port-number, port-name=port-number, ...*}** – assign ports to services for this instance. Use only with **-create** or **-refresh**. For the *port-name* value, use a port name from the table below. If you plan to run more than one SCC instance on a host machine, you must reassign all the ports for every instance after the first.

Port information:

Port Name	Description	Service Names	Property Names	Default Port
db	Database port Present on SCC server	SccSADataserver Messaging Alert Scheduler	com.sybase.asa.server.port messaging.db.port alert.database.port org.quartz.data-Source.ASA.URL	3638
http	Web HTTP port Present on SCC server	EmbeddedWebCon- tainer	http.port	8282
https	Web HTTPS (secure HTTP) port Present on SCC server	EmbeddedWebCon- tainer	https.port	8283
jiniHttp	JINI HTTP server Present on SCC server and SCC agent	Jini	httpPort	9092
jiniR- mid	JINI remote method in- vocation daemon Present on SCC server and SCC agent	Jini	rmidPort	9095
msg	Messaging port Present on SCC server	Messaging	messaging.port	2000
rmi	RMI port Present on SCC server and SCC agent	RMI	port	9999
tds	Tabular Data Stream™ port (used to communi- cate with other Sybase products) Present on SCC server and SCC agent	Tds	tdsPort	9998

- **-refresh** – recopy all the files that make up this instance (Windows) or all this instance's services and plug-ins (UNIX). Refreshing preserves any service or plug-in configuration in the deployed instance.

You can also use **-refresh** to convert a server to an agent or an agent to a server (see the examples). Files are removed or added to change the function of the instance. Use alone or

with **-agent** to refresh an agent instance, or with **-server** to refresh a server instance. Generates an error if the instance is running.

- **-r | -remove** – delete an instance. Use alone or with **-instance**. Generates an error if the instance is running. You cannot restore a removed instance.
- **-s | -server** – use with **-create** or **-refresh** to create or refresh an SCC server, including any product modules available.
- **-service** – use with **-create** or **-remove** to create or remove a Windows service for this instance. You must be logged in to Windows as an administrator to use this option.
- **-silent** – suppress the output of **sccinstance**.

Examples

- **Deploy an SCC server instance** – enables shared-disk mode, deploys a server called Boston with a Windows service on the current host, and starts the Windows service:

```
sccinstance -enable  
sccinstance -create -server -instance Boston -service  
net start "Sybase Control Center 3.2.3 (Boston)"
```

Note: To create the service, you must log in to Windows as an administrator.

- **Deploy an SCC agent instance** – deploys an SCC agent on this host and configures a Windows service for it. The **-agent** option, because it is the default, is not required—the command does exactly the same thing without it.

```
sccinstance -create -agent -service
```

or

```
sccinstance -create -service
```

- **Deploy a server instance and reassign ports** – deploys the server on this host and configures nondefault RMI, HTTP, and HTTPS ports.

```
sccinstance -create -server -portconfig  
rmi=8888,http=7070,https=7071
```

- **Deploy two instances on the same host** – creates two agent instances on the host fireball. The first command does not need the **-host** option because the instance name is the same as the host name.

```
sccinstance -create -agent -instance fireball -portconfig rmi=9991  
sccinstance -create -agent -instance fireball2 -host fireball  
-portconfig rmi=9992
```

Note: In a production environment, Sybase recommends that you deploy no more than one SCC instance of each type (one server and one agent) on the same host.

- **Refresh a server instance or convert an agent to a server** – refreshes the server on this host. If the instance on this host is an SCC agent, refreshing it as an SCC server converts it into a server.

```
sccinstance -refresh -server
```

- **Refresh an agent instance or convert a server to an agent** – refreshes the instance named kalamazoo. If kalamazoo is a server, refreshing it as an SCC agent converts it into an agent.

```
sccinstance -refresh -agent -instance kalamazoo
```

- **Remove a server instance** – removes the instance named porcupine if it is not running:

```
sccinstance -remove -instance porcupine
```

- **Display status** – displays the status of the instance on this host:

```
sccinstance
```

- **List all instances** – displays a list of all SCC server and agent instances deployed from this SCC installation:

```
sccinstance -list
```

- **Scenario: Remove an instance by force** – suppose you have inadvertently deployed two SCC agent instances on the same host:

```
$ sccinstance -list
2 SCC instances deployed:
SCC instance node1 deployed in agent mode for host node1 RMI port
9999
SCC instance node2 deployed in agent mode for host node2 RMI port
9999
```

Both instances use the same RMI port. You must either reassign ports for one instance or remove it. But you get an error if you try remove an instance when another instance is running on the same host:

```
$ sccinstance -instance node2 -remove
[ERROR] Command execution failed.
[ERROR] SCC instance node2 could not be removed because it is
running. Shut
down the SCC before removing the instance.
```

Use the **-force** option to override the error and force the removal of the second agent instance:

```
$ sccinstance -instance node2 -remove -force
Removing SCC instance node2 ...
SCC instance node2 was successfully removed.
```

Permissions

sccinstance permission defaults to all users, except as noted for certain parameters.

See also

- *Enabling and Disabling Shared-Disk Mode* on page 74
- *Shared-Disk Mode* on page 74

Launching Sybase Control Center

Use the **scc** command to start Sybase Control Center.

Prerequisites

Install Adobe Flash Player in the browser you will use for Sybase Control Center.

Task

1. Start Sybase Control Center.

- Windows – navigate to `<install_location>\SCC-3_2\bin` and double-click **scc.bat**.
- UNIX – execute **scc.sh**.

Messages on the progress of the launch appear in a command window. When Sybase Control Center is running, the command window becomes the Sybase Control Center console; you can issue commands to get status information on SCC and its ports, plug-ins, and services.

2. Open a Web browser and enter `https://<hostname>:8283/scc`.

See also

- *Sybase Control Center Console* on page 1333

Registering the ODBC Driver in Windows

In Windows, run **scc.bat** with administrative privileges to register the ODBC driver.

When Sybase Control Center starts for the first time on a Windows machine, it registers its ODBC driver. Because the automatic registration of the ODBC driver edits the registry settings, you must execute **scc.bat** using elevated administrative privileges. If you launch for the first time without adequate privileges, Sybase Control Center generates an error and fails to start.

In Windows Vista, Windows 2008, and Windows 7, you must use the **Run as administrator** setting to launch Sybase Control Center even if you already have administrative privileges. This process is described below.

In other versions of Windows, you must be logged in as an administrator to start Sybase Control Center for the first time. You need not follow the steps below.

- 1.** In Windows Vista, Windows 2008, or Windows 7, open the Command Prompt window with administrative privileges:

- Select **Start > All Programs > Accessories**. Right-click **Command Prompt** and select **Run as administrator**.
- Alternatively, enter **cmd** in the Start Menu search box and press **Shift+Ctrl+Enter**.

2. Run **scc.bat**.

See also

- *Starting and Stopping Sybase Control Center in Windows* on page 81
- *Starting and Stopping Sybase Control Center in UNIX* on page 84
- *Configuring Memory Usage* on page 88
- *scc Command* on page 91

Starting and Stopping Sybase Control Center in Windows

There are several ways to start and stop Sybase Control Center or the SCC agent. You can start manually, which is useful for testing and troubleshooting, or set the service to start automatically and to restart in case of failure.

This topic applies to both Sybase Control Center (the server, which includes the management UI) and the Sybase Control Center agent that runs on each product server managed by SCC. When you install SCC and the SCC agent in the same directory by selecting both options in the installer, you start and stop them together—by executing a single command or controlling a single service. This topic applies both to singleton installations (which do not use a shared disk) and to instances of SCC agents and servers running from a shared disk.

If you run Sybase Control Center or the SCC agent manually, you must issue a command every time you start or shut down. If you run as a service (which is recommended), you can configure the service to start and restart automatically. These are the options:

- Use the **scc.bat** command to start Sybase Control Center or the SCC agent manually. The command gives you access to the Sybase Control Center console, which you can use to shut down and to display information about services, ports, system properties, and environment variables. You can also use **scc.bat** to change the logging level for troubleshooting purposes. Using **scc.bat** prevents you from taking advantage of the automatic start and restart features available to services.
- Use the Services list under the Windows Control Panel to start, stop, and configure the Sybase Control Center service for an SCC server or agent.
- Use the **net start** and **net stop** commands. This is another way to run Sybase Control Center or the SCC agent as a service.

Note: To start an SCC agent or server as a service:

- In a singleton installation, you must have selected **Yes** in the installer to install the agent or server as a service.
 - In a shared disk installation, the agent or server must have been deployed using the **-service** option of the **sccinstance** command.
-

Get Started

In a singleton installation, the installer lets you start Sybase Control Center or the SCC agent as a service and configures the service to restart automatically. Before starting, check the Windows Services list for a Sybase Control Center service.

Here are the steps for each starting and stopping option:

- **Start Sybase Control Center, the SCC agent, or both when they are installed together:**

- a) (Skip this step for the SCC agent.) If you are starting Sybase Control Center for the first time in Windows Vista, Windows 2008, or Windows 7, set the **Run as Administrator** option on the command prompt so that Sybase Control Center can register its ODBC driver. (This is necessary even if you are logged in as an administrator.)

- b) Enter the **scc** command.

For a singleton installation:

```
%SYBASE%\SCC-3_2\bin\scc.bat
```

For an instance:

```
%SYBASE%\SCC-3_2\bin\scc.bat -instance <instance-name>
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

- **Stop Sybase Control Center, the SCC agent, or both when they are installed together:**

- a) Enter the **scc --stop** command.

For a singleton installation:

```
%SYBASE%\SCC-3_2\bin\scc.bat --stop
```

For an instance:

```
%SYBASE%\SCC-3_2\bin\scc.bat --stop -instance <instance-name>
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

Note: You can also enter **shutdown** at the `scc-console>` prompt.

- **Start or stop from the Windows Control Panel; configure automatic start and restart:**

- a) Open the Windows Control Panel.
- b) Select **Administrative Tools > Services**.
- c) Locate "Sybase Control Center" in the Services list. It may be followed by a release number; if the service is for an instance, it is also followed by the instance name.

Service names do not distinguish between agents and servers. If the service is running, the Status column displays “Started.”

- d) To start or stop the service, right-click the **Sybase Control Center** entry in the Services list and choose **Start** or **Stop**.
- e) To configure automatic starting, double-click the service.
- f) To set the service to automatically start when the machine starts, change the **Startup type** to Automatic.
- g) To restart the service in case of failure, choose the **Recovery** tab and change the First, Second, and Subsequent failures to Restart Service.
- h) Click **Apply** to save the modifications and close the dialog.
- **Start or stop the Sybase Control Center service (controlling Sybase Control Center, the SCC agent, or both) from the Windows command line:**
 - a) To start the service, enter the **net start** command.

For a singleton installation:

```
net start "sybase control center 3.2.8"

The Sybase Control Center 3.2.8 service is starting.....
The Sybase Control Center 3.2.8 service was started
successfully.
```

For an instance, include the instance name (Boston-1 in this example) in parentheses:

```
net start "sybase control center 3.2.8 (Boston-1) "

The Sybase Control Center 3.2.8 (Boston-1) service is
starting.....
The Sybase Control Center 3.2.8 (Boston-1) service was
started successfully.
```

- b) To stop the service, enter the **net stop** command.

For a singleton installation:

```
net stop "sybase control center 3.2.8"

The Sybase Control Center 3.2.8 service is stopping.....
The Sybase Control Center 3.2.8 service was stopped
successfully.
```

For an instance, include the instance name (Boston-1 in this example) in parentheses:

```
net stop "sybase control center 3.2.8 (Boston-1) "

The Sybase Control Center 3.2.8 (Boston-1) service is
stopping.....
The Sybase Control Center 3.2.8 (Boston-1) service was
stopped successfully.
```

See also

- *Registering the ODBC Driver in Windows* on page 80
- *Starting and Stopping Sybase Control Center in UNIX* on page 84
- *Configuring Memory Usage* on page 88
- *scc Command* on page 91

Starting and Stopping Sybase Control Center in UNIX

You can start Sybase Control Center or the SCC agent manually, which is useful for testing and troubleshooting, or you can set up a service to start automatically and to restart in case of failure.

This topic applies to both Sybase Control Center (the server, which includes the management UI) and the Sybase Control Center agent that runs on each product server managed by SCC.. When you install SCC and the SCC agent in the same directory by selecting both options in the installer, you start and stop them together—by executing a single command or controlling a single service. This topic applies to both singleton installations (which do not use a shared disk) and instances of SCC agents and servers running from a shared disk.

If you start Sybase Control Center or the SCC agent manually, you must issue a command every time you start or shut down. If you run as a service (which is recommended), you can configure the service to start and restart automatically. These are the options:

- Use the **scc.sh** script to start Sybase Control Center or the SCC agent manually. You can either:
 - Run **scc.sh** in the foreground to get access to the Sybase Control Center console, which you can use to shut down and to display information about services, ports, system properties, and environment variables.
 - Run **scc.sh** in the background to suppress the console.You can use **scc.sh** to run Sybase Control Center at a nondefault logging level for troubleshooting. When you start manually with **scc.sh**, you cannot take advantage of the automatic start and restart features available to services.
- Use the **sccd** script to configure a service that starts Sybase Control Center or the SCC agent automatically.

Here are the steps for each starting and stopping option:

- **Before you start Sybase Control Center or the SCC agent for the first time, set environment variables.** Do this only once.
 - a) Change to the Sybase directory (the parent of the Sybase Control Center installation directory).
 - b) Execute one of the following to set environment variables.

Bourne shell:

```
. SYBASE.sh
```

C shell:

```
source SYBASE.csh
```

- **Run Sybase Control Center or the SCC agent (or both, when they are installed together) in the foreground.**

Running in the foreground is a method of manually starting; you must issue commands to stop and restart Sybase Control Center or the SCC agent.

- a) To start Sybase Control Center or the SCC agent and drop into the console when the start-up sequence is finished, enter the **scc** command.

For a singleton installation:

```
$SYBASE/SCC-3_2/bin/scc.sh
```

For an instance:

```
$SYBASE/SCC-3_2/bin/scc.sh -instance <instance-name>
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

- **Run Sybase Control Center or the SCC agent (or both, when they are installed together) in the background.**

You can use **nohup**, **&**, and **>** to run Sybase Control Center or the SCC agent in the background, redirect output and system error to a file, and suppress the SCC console. Running in the background is a method of manually starting; you must issue commands to stop and restart Sybase Control Center or the SCC agent.

- a) Execute a command similar to the sample below that matches your shell. Both sample commands direct output to the file `scc-console.out`. If the output file already exists, you might need to use additional shell operators to append to or truncate the file.

Bourne shell (sh) or Bash

For a singleton installation:

```
nohup ./scc.sh 2>&1 > scc-console.out &
```

For an instance:

```
nohup ./scc.sh -instance <instance-name> 2>&1 > scc-console-  
your-instance.out &
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

C shell

For a singleton installation:

```
nohup ./scc.sh >& scc-console.out &
```

For an instance:

```
nohup ./scc.sh -instance <instance-name> >& scc-console.out &
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

- **Shut down Sybase Control Center or the SCC agent (or both, when they are installed together) .**

a) To shut down from the `scc-console>` prompt, enter:

```
shutdown
```

Warning! Do not enter **shutdown** at a UNIX prompt; it shuts down the operating system.

To shut down from the UNIX command line, enter the **scc --stop** command.

For a singleton installation:

```
$SYBASE/SCC-3_2/bin/scc.sh --stop
```

For an instance:

```
$SYBASE/SCC-3_2/bin/scc.sh --stop -instance <instance-name>
```

You can omit the **-instance** option if the instance's name is the same as its host name (the default).

- **Configure Sybase Control Center or the SCC agent to run as a service.**

A UNIX service is a daemon process that starts automatically after the machine is started and runs in the background. UNIX installations of Sybase Control Center include a shell script, **sccd**, which you can use to configure the Sybase Control Center service. (Some UNIX platforms supply tools that make service configuration easier; Linux **chkconfig** is an example.)

Note: Sybase recommends that if you are not familiar with setting up services in UNIX, you delegate this task to a system administrator or consult the system administration documentation for your UNIX platform.

a) Copy `$SYBASE/SCC-3_2/bin/sccd` into this directory:

- AIX (SCC agent only): `/etc/rc.d/init.d`
- HP-UX (SCC agent only): `/sbin/init.d`
- All other platforms: `/etc/init.d`

b) Open `sccd` and make these changes:

- Change the line that sets the SYBASE variable to the location of your Sybase installation (that is, the parent of `SCC-3_2`, the Sybase Control Center installation directory). By default, this directory is called `Sybase`.
- If you are not using shared-disk mode, or you are using shared-disk mode to run a single instance whose name is the same as the host name, skip to step 5.c on page 87 or step 5.d on page 87.

- If you are using shared-disk mode to run a single instance whose name is not the host name, or to run multiple instances on the same host, add the instance name to the script name. Change:

```
SCRIPT_NAME=scc.sh
```

to:

```
SCRIPT_NAME="scc.sh -instance <instance-name>"
```

- If you are using shared-disk mode to run multiple instances on the same host, append the instance name to the name of the output log file. Change:

```
./${SCRIPT_NAME} --start 2>&1 >> ${SCC_HOME}/log/scc-  
service.out &
```

to:

```
./${SCRIPT_NAME} --start 2>&1 >> ${SCC_HOME}/log/scc-  
service_<instance-name>.out &
```

- If you are using shared-disk mode to run multiple instances on the same host, save a copy of the `sccd` script for each instance, giving each copy a unique name. In each copy, add the instance name to the script name and append the instance name to the output log file name as described above. Perform the remaining steps in this procedure for each copy of `sccd`.

- c) In Linux, configure the service to run in run levels 2, 3, 4, and 5:

```
/usr/sbin/chkconfig --add sccd  
/usr/sbin/chkconfig --level 2345 sccd
```

You can test the `sccd` script with `/usr/sbin/service sccd status`. (The **service** command accepts these options: **start** | **stop** | **status** | **restart**.)

- d) On non-Linux platforms, locate this directory:

- AIX (SCC agent only): `/etc/rc.d/rc<X>.d`
- HP-UX (SCC agent only): `/sbin/rc<X>.d`
- Solaris: `/etc/rc<X>.d`

where `<X>` is the run level (for example, 3). Make two soft links in the directory for your platform and set the links to point to:

- AIX (SCC agent only):
`/etc/rc.d/init.d/sccd: S90sccd` and
`/etc/rc.d/init.d/sccd: K10sccd`
- HP-UX (SCC agent only):
`/sbin/init.d/sccd: S90sccd` and
`/sbin/init.d/sccd: K10sccd`
- Solaris:
`/etc/init.d/sccd: S90sccd` and
`/etc/init.d/sccd: K10sccd`

The `S90sccd` link starts the service and the `K10sccd` link stops the service. The two-digit numbers in the links indicate the start and stop priorities of the service.

- e) Use the `S90sccd` and `K10sccd` links to test starting and stopping the service. The links are called automatically when the machine is started or shut down.

See also

- *Registering the ODBC Driver in Windows* on page 80
- *Starting and Stopping Sybase Control Center in Windows* on page 81
- *Configuring Memory Usage* on page 88
- *scc Command* on page 91

Configuring Memory Usage

(Optional) Determine whether you need to configure how much memory Sybase Control Center uses, and if so which configuration method to use.

It is not usually necessary to configure memory usage for Sybase Control Center. This table lists memory options you can set and circumstances under which you should consider changing them.

Modify this value	When	Guidelines
<p>Maximum memory</p> <ul style="list-style-type: none"> • <code>jvmopt=-Xmx</code> – if you are running Sybase Control Center as a Windows service • <code>SCC_MEM_MAX</code> – if you are running SCC as a UNIX service • <code>SCC_MEM_MAX</code> – if you are starting SCC from the command line 	<ul style="list-style-type: none"> • You need to prevent Sybase Control Center from using more than a given amount of memory • Sybase Control Center fails to start and may display an error: <code>Could not create the Java Virtual machine.</code> • An <code>OutOfMemory</code> error says Sybase Control Center is out of heap space • A warning message about system memory appears during the start process • The machine where Sybase Control Center is installed has less than 4GB of memory. (Starting Sybase Control Center on a machine with less than 4GB of memory triggers the startup warning message about system memory.) 	<p>On machines with less than 4GB of memory, set maximum memory to 256MB or more.</p> <p>Default value: none. (On machines with 4GB or more of memory, maximum memory is set dynamically and is effectively limited only by the amount of system memory available.)</p>

Modify this value	When	Guidelines
Permanent memory <ul style="list-style-type: none"> • <code>jvmopt=-XX:MaxPermSize</code> – if you are running Sybase Control Center as a Windows service • <code>SCC_MEM_PERM</code> – if you are running SCC as a UNIX service • <code>SCC_MEM_PERM</code> – if you are starting SCC from the command line 	An OutOfMemory error says Sybase Control Center is out of permanent generation space	Increase by 32MB increments. If you reach a value equal to twice the default and still see the OutOfMemory error, contact Sybase technical support. Default value: 128MB

You can change memory options in two ways:

- For Sybase Control Center started from the command line – execute commands to set one or more environment variables before executing the **scc** command to start Sybase Control Center. When you use this method, your changes to the memory options last only as long as the current login session. This method is useful for testing new option values.
- For the Sybase Control Center service – modify a file used by the Sybase Control Center service. When you use this method, your changes to the memory options persist—Sybase Control Center uses them every time it starts as a service.

See also

- *Registering the ODBC Driver in Windows* on page 80
- *Starting and Stopping Sybase Control Center in Windows* on page 81
- *Starting and Stopping Sybase Control Center in UNIX* on page 84
- *scc Command* on page 91

Changing a Memory Option on the Command Line

Before you start Sybase Control Center from the command line, you can issue a command to change the value of a memory option temporarily.

Changes made using this method last only as long as the current login session. This method is useful for testing new option values.

1. If Sybase Control Center is running, shut it down.
2. Set the environment variable. Specify a size in megabytes but do not indicate the units in the command.

Windows example:

Get Started

```
> set SCC_MEM_MAX=512
```

UNIX example:

```
bash$ export SCC_MEM_MAX=512
```

3. Use the **scc** command to start Sybase Control Center.

See also

- *Changing a Memory Option for a Sybase Control Center Windows Service* on page 90
- *Changing a Memory Option for an SCC UNIX Service* on page 90
- *Starting and Stopping Sybase Control Center in Windows* on page 81
- *Starting and Stopping Sybase Control Center in UNIX* on page 84
- *scc Command* on page 91

Changing a Memory Option for a Sybase Control Center Windows Service

Add a **jvmopt** command to the `scc.properties` file to change a memory option (`-Xmx` or `-XX:MaxPermSize`) for a Sybase Control Center Windows service.

When you use this method to set memory options, your changes are permanent—Sybase Control Center uses them every time it starts as a service.

1. If Sybase Control Center is running, shut it down.
2. Open the Sybase Control Center properties file:
`<Sybase Control Center-install-directory>\SCC-3_2\bin
\scc.properties`
3. Add (or modify, if it already exists) a **jvmopt** line specifying the memory size in Java format. Use `m` for megabytes or `g` for gigabytes.

For example:

```
jvmopt=-Xmx512m
```

4. Save the file and start the Sybase Control Center Windows service.

See also

- *Changing a Memory Option on the Command Line* on page 89
- *Changing a Memory Option for an SCC UNIX Service* on page 90
- *Starting and Stopping Sybase Control Center in Windows* on page 81

Changing a Memory Option for an SCC UNIX Service

To change a memory setting for a Sybase Control Center UNIX service, add the appropriate environment variable (`SCC_MEM_MAX` or `SCC_MEM_PERM`) to the `sccd` script.

When you use this method to set memory options, your changes are permanent—Sybase Control Center uses them every time it starts as a service.

1. If Sybase Control Center is running, shut it down.
2. Open the sccd file: `/etc/init.d/sccd`
3. Add the environment variable at the top of the file (after the comments). Specify a size in megabytes but do not indicate the units in the command.

For example:

```
SCC_MEM_MAX=512
```

4. Save the file and start the Sybase Control Center UNIX service.

See also

- *Changing a Memory Option on the Command Line* on page 89
- *Changing a Memory Option for a Sybase Control Center Windows Service* on page 90
- *Starting and Stopping Sybase Control Center in UNIX* on page 84

scc Command

Use **scc.bat** (Windows) or **scc.sh** (UNIX) to start and stop Sybase Control Center agents and servers and to perform administrative tasks like configuring ports and enabling and disabling services.

Syntax

```
scc[.bat | .sh] [-a | --address RMI-service-address]
[-b | --bitwidth]
[--dbpassword]
[-disable | --disable service-name,service-name...]
[-enable | --enable service-name,service-name...]
[-h | --help]
[-I | --info [information-category]]
[-instance [instance-name]]
[-m | --message message-level]
[-password | --password password]

[-p | --port {port-name=port-number |
               service-name:property-name=port-number}]
[{-start | --start} | {-stop | --stop}]
[-status | --status]
[-user | --user login-name]
[-v | -version | --version]
```

Parameters

- **-a | --address *RMI-service-address*** – the address for the RMI service to use; must be an IP address on this machine or the name of this machine (which is the default).
- **-b | --bitwidth** – returns a string identifying the bit width (32 or 64) of the underlying platform; Sybase Control Center uses this option to determine which libraries to use for its internal database. If you use this option, the **scc** command does not start Sybase Control Center.

- **--dbpassword** – changes the password of the default dba account provided for the repository database. It prompts you for the new password, validates it, and starts the Sybase Control Center server. This option does not work if you start Sybase Control Center in the background—the server fails to start if there is no console.
- **--disable** | **--disable *service-name,service-name...*** – disable the specified Sybase Control Center services. This option does not work while Sybase Control Center is running or as part of a command that starts SCC. To use it, shut down SCC, execute `scc --disable`, then restart. See under `--ports` for service names; separate each service from the next with a comma.
- **--enable** | **--enable *service-name,service-name...*** – enable the specified Sybase Control Center services. See under `--ports` for service names; separate each service from the next with a comma. When you use this option, **scc** does not start Sybase Control Center—use a separate command to start SCC.
- **-h** | **--help** – display help and usage information for the **scc** command. If you use this option, **scc** does not start Sybase Control Center.
- **-I** | **--info [*information-category*]** – display the specified categories of information about Sybase Control Center. Separate each category from the next with a comma. The information categories are:
 - **all** – returns all the information provided by the `sys`, `ports`, and `services` categories. Default option.
 - **sys** – returns general information about this instance of Sybase Control Center, including the version, the home (installation) directory, the host machine's name and IP address, the RMI port number, the messaging level, and details about the platform and Java installation.
 - **ports** – lists all the ports on which the Sybase Control Center agent and its services listen, indicates whether each port is in use, and shows the service running on each port.
 - **services** – lists all the services known to the Sybase Control Center agent, indicates whether each service is enabled, and lists other services on which each service depends.
 - **sysprop** – lists all the Java system properties known the Java VM and their values.
 - **env** – lists the complete Java VM process environment.
- **--instance [*instance-name*]** – use with other options (**--start** and **--stop**, for example) to specify a Sybase Control Center instance in a shared disk deployment. If you do not enter a name for the instance, it defaults to the host name.
- **-m** | **--message *message-level*** – set the amount of detail recorded in system logs; also known as the logging level. Valid values are OFF, FATAL, ERROR, WARN, INFO, DEBUG, and ALL. WARN is the default.
- **--password** | **--password** – specify the password of the user account Sybase Control Center will use to stop servers or query them for status. Use this option with **--user**. When you enter a command with **--user** but without **--password**, the console prompts you to enter a password.

- **-p | --port {port-name=port-number | service-name:property-name=port-number}** – configure the specified service to run on the specified port. Changing ports is useful if you discover a port conflict between Sybase Control Center and other software on the same system. When you use this option, **scc** does not start Sybase Control Center—use a separate command to start SCC.

Valid port names, service names and property names are:

Port Name	Description	Service Names	Property Names	Default Port
db	Database port Present on SCC server	SccSADataserver Messaging Alert Scheduler	com.sybase.asa.server.port messaging.db.port alert.database.port org.quartz.data-Source.ASA.URL	3638
http	Web HTTP port Present on SCC server	EmbeddedWebCon- tainer	http.port	8282
https	Web HTTPS (secure HTTP) port Present on SCC server	EmbeddedWebCon- tainer	https.port	8283
jiniHttp	JINI HTTP server Present on SCC server and SCC agent	Jini	httpPort	9092
jiniR- mid	JINI remote method in- vocation daemon Present on SCC server and SCC agent	Jini	rmidPort	9095
msg	Messaging port Present on SCC server	Messaging	messaging.port	2000
rmi	RMI port Present on SCC server and SCC agent	RMI	port	9999
tds	Tabular Data Stream™ port (used to communi- cate with other Sybase products) Present on SCC server and SCC agent	Tds	tdsPort	9998

You can also execute `scc --info ports` to display service names and associated property names; they appear in the first two columns of the output.

- **-start | --start** – start the Sybase Control Center server. This is the default option—if you execute **scc** with no options, it starts SCC. This option cannot be combined in the same command with options that set ports or enable or disable services; use a separate **scc** command to start SCC.
- **-status | --status** – display a status message indicating whether the Sybase Control Center server is running.
- **-stop | --stop** – shut down the Sybase Control Center server if it is running.
- **-user | --user [login-name]** – specify the user account Sybase Control Center will use to stop managed servers or query them for status. Use this option with **--password**. If you do not enter a login name, the console prompts you to enter one.
- **-v | --version | --version** – display the version of Sybase Control Center software running on this server. If you use this option, **scc** does not start Sybase Control Center.

Examples

- **Set the RMI port** – each of these commands sets the RMI port to 9999 (the default). The first command illustrates the port name syntax; the second illustrates the service name:property name syntax.

```
scc --port rmi=9999
scc --port RMI:port=9999
```

- **Set the RMI port and start SCC** – these commands set the RMI port to 9996, then start SCC. Two commands (separated by a semicolon here) are needed because **scc** does not start Sybase Control Center when it includes any of the port-setting options.

```
scc -p rmi=9996; scc
```

- **Set all database ports** – this command sets all four of the SQL Anywhere database ports (data server, messaging, database alert, and scheduler) to 3638. (SQL Anywhere is the Sybase Control Center internal repository.)

```
scc --port db=3638
```

- **Set the TDS port** – this command sets the TDS port to 9998 (the default):

```
scc --port Tds:tdsPort=9998
```

- **Enable a service and start SCC** – the first **scc** command enables the TDS service; the second starts SCC. (The two commands are separated by a semicolon.) The second command is needed because **scc** does not start Sybase Control Center when it includes the **-enable** option.

```
scc -enable Tds; scc
```

- **Start an SCC instance** – this command starts the SCC instance called kalamazoo. **-start** is optional because it is the default.

```
scc -start -instance kalamazoo
```

Permissions

scc permission defaults to all users. No permission is required to use it.

See also

- *Registering the ODBC Driver in Windows* on page 80
- *Starting and Stopping Sybase Control Center in Windows* on page 81
- *Starting and Stopping Sybase Control Center in UNIX* on page 84
- *Configuring Memory Usage* on page 88
- *Configuring Ports* on page 114
- *Logging or Message Levels* on page 1331

Logging in to Sybase Control Center

Enter the Sybase Control Center Web console.

Prerequisites

Install Adobe Flash Player in the browser you will use for SCC. See the *Sybase Control Center Installation Guide*.

Task

Sybase Control Center typically authenticates users through the operating system or an LDAP directory service. Consult your SCC administrator if you are not sure which login account to use for SCC.

Only one login session per account is permitted at a time; multiple users cannot be logged in to the same account simultaneously.

Note: When logging in to a newly installed Sybase Control Center for which secure authentication has not been configured, use the `sccadmin` account—the password is set during installation. For more information, see the *Sybase Control Center Installation Guide*.

1. Connect to the Sybase Control Center server. In your Web browser, enter: `https://scc-hostname:8283/scc`.
2. Enter your user name and password, and click **Login**.

Tip: If you use a Windows account to log in to SCC, enter your user name in the format `username@domain`. Omit top-level domain extensions such as `.com` or `.net`—for example, enter `fred@sap`, not `fred@sap.com`.

See also

- *Logging out of Sybase Control Center* on page 96

Logging out of Sybase Control Center

When you finish working in Sybase Control Center, end your login session.

From the main menu bar, select **Application > Log Out**.

Alternatively, click **Log Out** in the upper-right corner of the window.

Note: If an administrator has configured the automatic logout feature, Sybase Control Center logs you out if your session is idle (no typing or mouse movement) for longer than the timeout period, which is set by the administrator.

If no automatic logout period is configured,

- A login session left open on a screen that refreshes (a monitor screen or a data collection job screen, for example) remains open indefinitely.
 - A login session left open on a screen that does not change expires after 30 minutes. The next time you make a request of the server, SCC logs you out.
-

See also

- *Logging in to Sybase Control Center* on page 95

Setting Up Security

Configure login authentication and map roles.

Read about security and follow these procedures before you configure Sybase Control Center product modules.

Note: These security topics are intended for use in a production environment. If you are evaluating or testing SCC, see *Quick Start for an Evaluation* on page 17.

1. *Security*

Sybase Control Center can authenticate user logins through an LDAP server, through the operating system, or both.

2. *Configuring Authentication for Windows*

Authentication through the Windows operating system is enabled by default.

Configuration is required only if you have upgraded from an older version of Sybase Control Center and no longer want to use the older version's authentication settings; if you

do not want to use Windows for authentication; or if you want to create login accounts manually. Sybase recommends that you allow SCC to create accounts automatically.

3. *Configuring a Pluggable Authentication Module (PAM) for UNIX*

Set up Sybase Control Center to support username and password login using accounts on the UNIX operating system.

4. *Configuring an LDAP Authentication Module*

Configure an LDAP authentication module for Sybase Control Center by editing the security configuration file to point to the correct LDAP server.

5. *Mapping Sybase Control Center Roles to LDAP or OS Groups*

To grant Sybase Control Center privileges to users who are authenticated through LDAP or the operating system, associate roles used in Sybase Control Center with groups in LDAP or the operating system.

6. *Encrypting a Password*

Use the `passencrypt` utility to encrypt passwords and other values that must be kept secure while stored in text files.

7. *Configuring Ports*

(Optional) Use the `scc --port` command to assign Sybase Control Center services to new ports.

Security

Sybase Control Center can authenticate user logins through an LDAP server, through the operating system, or both.

- Sybase Control Center can be configured to authenticate through any LDAP server that supports the `inetOrgPerson` (RFC 2798) schema.
- When Sybase Control Center authenticates through the operating system, it uses the operating system of the Sybase Control Center server machine (not the client).

Although you can create native user accounts in Sybase Control Center, Sybase does not recommend this approach to authentication. It is simpler and safer to configure Sybase Control Center to authenticate using existing LDAP, Windows, or UNIX login accounts.

Sybase strongly recommends that you use a common authentication provider for all Sybase products, including Sybase Control Center. A common authentication provider ensures that single sign-on works for users of Sybase Control Center and its managed servers.

Sybase Control Center requires each authenticated login account to have a predefined role. When a login is authenticated, roles for the login are retrieved by the security module and are mapped to Sybase Control Center predefined roles. Authorization is resolved through the mappings between the security module native roles and Sybase Control Center roles. You can enable mappings by creating a “sybase” group in your operating system or LDAP server and adding all Sybase Control Center users, or by modifying the Sybase Control Center `role-mapping.xml` file to configure the mapping of native roles to Sybase Control Center roles. The security module authenticates the logins and authorizes access to managed resources.

Sybase Control Center provides a set of predefined login modules for authentication. All login modules are defined in the `<install_location>/SCC-3_2/conf/csi_config.xml` file. The syntax is defined by the Sybase Common Security Infrastructure (CSI) framework. You can configure the different login modules to customize security strength. The login modules are:

- Preconfigured user login – defines a user name, password, and a list of roles. The default user name is `sccadmin`; its password is configured during installation and its native role is SCC Administrator, which maps to `sccAdminRole`. You can create additional accounts by adding preconfigured user login modules to `csi_config.xml`. However, Sybase does not recommend the use of preconfigured user login modules for authentication in production environments.
- NT proxy login – delegates authentication to the underlying Windows operating system. When you log in to Sybase Control Center through an NT Proxy Login module, enter your user name in the format `username@nt-domain-name`. For example, `user@sybase`. Windows authentication is enabled by default, but it requires some configuration after an upgrade from SCC 3.2.5 or earlier.
- UNIX proxy login – delegates authentication to the underlying UNIX or Linux operating system using Pluggable Authentication Modules (PAM). When you log in to Sybase Control Center through a UNIX PAM, enter your UNIX user name and password. UNIX authentication is enabled by default, but it requires some configuration.
- LDAP login – delegates authentication to an LDAP server you specify. When you log in to Sybase Control Center through an LDAP server, enter your LDAP user name and password. LDAP authentication is not enabled by default; you must configure the login module.

See also

- *Configuring a Pluggable Authentication Module (PAM) for UNIX* on page 49
- *Configuring an LDAP Authentication Module* on page 101
- *Mapping Sybase Control Center Roles to LDAP or OS Groups* on page 111

Configuring Authentication for Windows

Authentication through the Windows operating system is enabled by default. Configuration is required only if you have upgraded from an older version of Sybase Control Center and no longer want to use the older version's authentication settings; if you do not want to use Windows for authentication; or if you want to create login accounts manually. Sybase recommends that you allow SCC to create accounts automatically.

This task is optional. However, if you choose not to create Sybase Control Center accounts automatically, you must enter them manually. Even when SCC users authenticate through LDAP or the local operating system, SCC needs the accounts for purposes of setting authorization (user privileges).

1. Log in to Sybase Control Center using an account with administrative privileges. (The login account or its group must have sccAdminRole.)
2. Select **Application > Administration > Security**.
3. Click to select or deselect the box labeled **Automatically add SCC login records for authenticated logins**.
4. Click to select or deselect the box labeled **Automatically grant sccUserRole to newly created logins**.
5. Click **OK** to close the Security dialog.

Next

There are two next steps:

- If you opted not to automatically create Sybase Control Center login accounts, enter each account into Sybase Control Center manually.
- Grant privileges to login accounts that require more than basic user access. You can grant privileges by assigning Sybase Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping Sybase Control Center roles to the groups. The group approach is generally more efficient.

See also

- *Configuring an LDAP Authentication Module* on page 101
- *Mapping Sybase Control Center Roles to LDAP or OS Groups* on page 111
- *Adding a Login Account to the System* on page 123

Configuring a Pluggable Authentication Module (PAM) for UNIX

Set up Sybase Control Center to support username and password login using accounts on the UNIX operating system.

1. Using a login account with root privileges, configure the pluggable authentication module for your platform:

Platform	Action
Solaris	Append the contents of the <SCC-install-dir>/utility/<su-nos>/pam.conf file (provided with Sybase Control Center) to the /etc/pam.conf file on your Solaris platform.

Platform	Action
Linux	Copy the <SCC-install-dir>/utility/<linux>/sybase-csi file (provided with Sybase Control Center) to the /etc/pam.d directory on your Linux platform. Note: The sybase-csi file provided with Sybase Control Center is not compatible with the most recent SUSE Linux versions. For SUSE 11 and later, see the example at the end of this topic.

Note: In the table above, the portion of the path that indicates the operating system might differ slightly from what is shown.

2. If the host UNIX system is not using a directory lookup for authentication (yp or NIS, for example) and authentication is carried out against the local /etc/passwd file, change the permissions on /etc/shadow to provide read access to the login account that executes SCC.
3. (Skip if you configured a PAM before starting Sybase Control Center) Restart Sybase Control Center.
4. (Optional) Change account creation options.
 - a) Log in to Sybase Control Center using an account with administrative privileges (sccAdminRole).
 - b) Select **Application > Administration > Security**.
 - c) Click to select or deselect the box labeled **Automatically add SCC login records for authenticated logins**. (By default, this option is enabled for SCC 3.2.6 and later.)
 - d) Click to select or deselect the box labeled **Automatically grant sccUserRole to newly created logins**. (By default, this option is enabled for SCC 3.2.6 and later.)
 - e) Click **OK** to close the Security dialog.

Example: PAM for SUSE Linux 11 and later

For SUSE 11 and later, do not use the sybase-csi file provided with Sybase Control Center. Instead, in your /etc/pam.d directory, create a sybase-csi file that contains:

```
# sybase-csi PAM Configuration (SUSE style)
auth      include      common-auth
account   include      common-account
password  include      common-password
session   include      common-session
```

Next

There are two next steps:

- If you opted not to automatically create Sybase Control Center login accounts, enter each account into Sybase Control Center manually. Sybase Control Center needs the accounts for purposes of setting authorization (user privileges).

- Grant privileges to login accounts that require more than basic user access. You can grant privileges by assigning Sybase Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping Sybase Control Center roles to the groups. The group approach is generally more efficient.

Configuring an LDAP Authentication Module

Configure an LDAP authentication module for Sybase Control Center by editing the security configuration file to point to the correct LDAP server.

1. Open the <SCC-install-dir>\conf\csi_config.xml file.
2. Uncomment the LDAP module in the configuration file by removing the surrounding <!-- and --> characters (or, if necessary, add an LDAP module to the file). The sample module below specifies the LDAP server that will provide user authentication.

The sample module shows the properties used for an OpenDS LDAP server. See the example at the end of this task for values that work for ActiveDirectory. Configuration properties you can use in the LDAP module are described in a subtopic.

```
<authenticationProvider controlFlag="sufficient"
name="com.sybase.security.ldap.LDAPLoginModule">
  <options name="BindDN" value="cn=Directory Manager"/>
  <options name="BindPassword" value="secret"/>
  <options name="DefaultSearchBase" value="dc=example,dc=com"/>
  <options name="ProviderURL" value="ldap://localhost:10389"/>
  <options name="ServerType" value="openldap"/>
</authenticationProvider>
<provider name="com.sybase.security.ldap.LDAPAuthenticator"
type="authenticator"/>
```

Note: Change only values shown in bold. If BindPassword is encrypted (which Sybase recommends), the line that defines it must include encrypted="true". The line should look similar to this:

```
<options name="BindPassword" encrypted="true"
value="lsnjikfwregfqr43hu5io..." />
```

3. Save the file.
4. If your LDAP server's SSL certificate is signed by a nonstandard certificate authority (for example, if it is a self-signed certificate), use the **keytool** utility to configure your JVM or JDK to trust the certificate. Execute a command similar to this:

Windows:

```
keytool -import -keystore %SYBASE_JRE7%\lib\security\cacerts -
file <your cert file and path>
-alias ldapcert -storepass changeit
```

UNIX:

```
keytool -import -keystore $SYBASE_JRE7/lib/security/cacerts -file
```

Get Started

```
<your cert file and path>  
-alias ldapcert -storepass changeit
```

LDAP Configuration Values for ActiveDirectory

For an ActiveDirectory server, use these values for configuration properties in your LDAP login module:

```
ServerType: msad2K  
DefaultSearchBase: dc=<domainname>,dc=<tld> or o=<company  
name>,c=<country code>  
                E.g. dc=sybase,dc=com or o=Sybase,c=us  
ProviderUrl: ldaps://<hostname>:<port>  
                E.g.: ldaps://myserver:636  
AuthenticationFilter: (&(userPrincipalName={uid})  
(objectclass=user))  
BindDN: <User with read capability for all users>  
BindPassword: <Password for BindDN user>  
RoleFilter: (|(objectclass=groupofnames) (objectclass=group))  
controlFlag: sufficient
```

Next

Map Sybase Control Center roles to LDAP groups.

See also

- *Mapping Sybase Control Center Roles to LDAP or OS Groups* on page 111

LDAP Configuration Properties

Use these properties in your `csi_config.xml` file to control the Sybase Control Center LDAP service.

Note: These characters have special meaning when they appear in a name in LDAP: , (comma), = (equals), + (plus), < (less than), > (greater than), # (number or hash sign), ; (semicolon), \ (backslash), / (forward slash), LF (line feed), CR (carriage return), " (double quotation mark), ' (single quotation mark), * (asterisk), ? (question mark), & (ampersand), and a space at the beginning or end of a string. LDAP providers do not handle these special characters in any of the names or DN's in any of the configuration properties. Additionally, some of the properties, as identified below, cannot use these special characters in common names.

Property	Default Value	Description
ServerType	None	<p>Optional. The type of LDAP server you are connecting to:</p> <ul style="list-style-type: none"> • sunone5 -- SunOne 5.x OR iPlanet 5.x • msad2k -- Microsoft Active Directory, Windows 2000 • nsds4 -- Netscape Directory Server 4.x • openldap -- OpenLDAP Directory Server 2.x <p>The value you choose establishes default values for these other authentication properties:</p> <ul style="list-style-type: none"> • RoleFilter • UserRoleMembership • RoleMemberAttributes • AuthenticationFilter • DigestMD5Authentication • UseUserAccountControl
ProviderURL	ldap://local-host:389	<p>The URL used to connect to the LDAP server. Use the default value if the server is:</p> <ul style="list-style-type: none"> • Located on the same machine as your product that is enabled with the common security infrastructure. • Configured to use the default port (389). <p>Otherwise, use this syntax for setting the value:</p> <p>ldap://<hostname>:<port></p>

Property	Default Value	Description
DefaultSearchBase	None	<p>The LDAP search base that is used if no other search base is specified for authentication, roles, attribution, and self registration:</p> <ol style="list-style-type: none"> 1. <code>dc=<domainname>,dc=<tld></code> For example, a machine in the sybase.com domain would have a search base of <code>dc=sybase,dc=com</code>. 2. <code>o=<company name>,c=<country code></code> For example, this might be <code>o=Sybase,c=us</code> for a machine within the Sybase organization. <hr/> <p>Note: When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> • Do not use special characters, as listed above, in common names or distinguished names in the value of this property. • Do not use Chinese or Japanese characters in user names or passwords of this property.
SecurityProtocol	None	<p>The protocol to be used when connecting to the LDAP server.</p> <p>To use an encrypted protocol, use <code>ssl</code> instead of <code>ldaps</code> in the URL.</p>
AuthenticationMethod	Simple	<p>The authentication method to use for all authentication requests into LDAP. Legal values are generally the same as those of the <code>java.naming.security.authentication</code> JNDI property. Choose one of:</p> <ul style="list-style-type: none"> • <code>simple</code> — For clear-text password authentication. • <code>DIGEST-MD5</code> — For more secure hashed password authentication. This method requires that the server use plain text password storage and only works with JRE 1.4 or later.

Property	Default Value	Description
AuthenticationFilter	<p>For most LDAP servers: (&uid={uid})(objectclass=person))</p> <p>or</p> <p>For Active Directory e-mail lookups: (&userPrincipalName={uid})(objectclass=user)[ActiveDirectory]</p> <p>For Active Directory Windows user name lookups: (&sAMAccountName={uid})(objectclass=user)</p>	<p>The filter to use when looking up the user.</p> <p>When performing a user name based lookup, this filter is used to determine the LDAP entry that matches the supplied user name.</p> <p>The string "{uid}" in the filter is replaced with the supplied user name.</p> <hr/> <p>Note: When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> Do not use special characters, as listed above, in common names or distinguished names in the value of this property. Do not use Chinese or Japanese characters in user names or passwords of this property. <hr/>
AuthenticationScope	onelevel	<p>The authentication search scope. The supported values for this are:</p> <ul style="list-style-type: none"> onelevel subtree <p>If you do not specify a value or if you specify an invalid value, the default value is used.</p>

Property	Default Value	Description
AuthenticationSearchBase	None	<p>The search base used to authenticate users. If this property is not configured, the value for DefaultSearchBase is used.</p> <hr/> <p>Note: When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> • Do not use special characters, as listed above, in common names or distinguished names in the value of this property. • Do not use Chinese or Japanese characters in user names or passwords of this property. <hr/>
BindDN	None	<p>The user DN to bind against when building the initial LDAP connection.</p> <p>In many cases, this user may need read permissions on all user records. If you do not set a value, anonymous binding is used. Anonymous binding works on most servers without additional configuration.</p> <p>However, the LDAP attributer may use this DN to create users in the LDAP server. When the self-registration feature is used, this user may need permissions to create a user record. This behavior may occur if you do not set useUserCredentialsToBind to true. In this case, the LDAP attributer uses this DN to update the user attributes.</p>

Property	Default Value	Description
BindPassword	None	<p>The password for BindDN, which is used to authenticate any user. BindDN and BindPassword separate the LDAP connection into units.</p> <p>The AuthenticationMethod property determines the bind method used for this initial connection.</p> <p>Sybase recommends that you encrypt passwords, and provides a password encryption utility. If you encrypt BindPassword, include <code>encrypted=true</code> in the line that sets the option. For example:</p> <pre><options name="BindPassword" encrypted="true" value="lsnjikf-wregfqr43hu5io..." /></pre> <p>If you do not encrypt BindPassword, the option might look like this:</p> <pre><options name="BindPassword" value="s3cr3T" /></pre>
RoleSearchBase	None	<p>The search base used to retrieve lists of roles. If this property is not configured, LDAP uses the value for DefaultSearchBase.</p> <hr/> <p>Note: When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> Do not use special characters, as listed above, in common names or distinguished names in the value of this property. Do not use Chinese or Japanese characters in user names or passwords of this property. <hr/>

Property	Default Value	Description
RoleFilter	<p>For SunONE/iPlanet: (& (object-class=ldapsubentry) (object-class=nsroledefinition))</p> <p>For Netscape Directory Server: ((object-class=groupofnames) (object-class=groupofuniquenames))</p> <p>For ActiveDirectory: ((object-class=groupofnames) (object-class=group))</p>	<p>The role search filter. This filter should, when combined with the role search base and role scope, return a complete list of roles within the LDAP server. There are several default values, depending on the chosen server type. If the server type is not chosen and this property is not initialized, no roles are available.</p> <hr/> <p>Note: When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> Do not use special characters, as listed above, in common names or distinguished names in the value of this property. Do not use Chinese or Japanese characters in user names or passwords of this property. <hr/>
RoleMemberAttributes	For Netscape Directory Server and OpenLDAP Server: member,unique-member	<p>A comma-separated list of role attributes from which LDAP derives the DN's of users who have this role.</p> <p>These values are cross-referenced with the active user to determine the user's role list. One example of the use of this property is when using LDAP groups as placeholders for roles. This property has a default value only when the Netscape server type is chosen.</p>
RoleNameAttribute	cn	The attribute of the role entry used as the role name. This is the role name displayed in the role list or granted to the authenticated user.
RoleScope	onelevel	<p>The role search scope. Supported values include:</p> <ul style="list-style-type: none"> onelevel subtree <p>If you do not specify a value or if you specify an invalid value, LDAP uses the default value.</p>

Property	Default Value	Description
SkipRoleLookup	false	<p>Set this property to true to grant the roles looked up using the attributes specified by the property UserRoleMembershipAttributes without cross-referencing them with the roles looked up using the RoleSearchBase and RoleFilter.</p> <p>LDAP configuration validation succeeds even when an error is encountered when listing all the available roles. The error is logged to the server log during validation but not reported in SCC, allowing the configuration to be saved. This has an impact when listing the physical roles for role mapping as well as in SCC. To successfully authenticate the user, set the SkipRoleLookup property to true.</p>
UserRoleMembershipAttributes	<p>For iPlanet/SunONE: nsRoleDN</p> <p>For Active Directory: memberOf</p> <p>For all others: none</p>	<p>Defines a user attribute that contains the DN's of all of the roles a user is a member of.</p> <p>These comma-delimited values are cross-referenced with the roles retrieved in the role search base and search filter to generate a list of user's roles.</p> <p>If the SkipRoleSearch property is set to true, these comma-delimited values are not cross-referenced with the roles retrieved in the role search base and role search filter. See <i>SkipRoleLookup</i>.</p> <hr/> <p>Note: If you use nested groups with Active Directory, you must set this property to tokenGroups.</p>
UserFreeformRoleMembershipAttributes	None	<p>The free-form role membership attribute list. Users who have attributes in this comma-delimited list are automatically granted access to roles whose names are equal to the attribute value. For example, if the value of this property is department and the department attribute in the user's LDAP record has the values {sales, consulting}, the user is granted the roles sales and consulting.</p>
Referral	ignore	<p>The behavior when a referral is encountered. Valid values are dictated by LdapContext, but might include follow, ignore, or throw.</p>

Property	Default Value	Description
DigestMD5Authentication-Format	DN For OpenLDAP: User name	The DIGEST-MD5 bind authentication identity format.
UseUserAccountControlAttribute	For Active Directory: true	When this property is set to true, the UserAccountControl attribute detects disabled user accounts, account expirations, password expirations, and so on. Active Directory also uses this attribute to store the above information.
EnableLDAPConnection-Trace	False	Enables LDAP connection tracing. The output is logged to a file in the temp directory. The location of the file is logged to the server log.
ConnectTimeout	0	Specifies the timeout, in milliseconds, for attempts to connect to the LDAP server. The property value sets the JNDI com.sun.jndi.ldap.connect.timeout property when attempting to establish a connection to a configured LDAP server. If the LDAP provider cannot establish a connection within the configured interval, it aborts the connection attempt. An integer value less than or equal to zero results in the use of the network protocol's timeout value.
ReadTimeout	0	Controls the length of time, in milliseconds, the client waits for the server to respond to a read attempt after the initial connection to the server has been established. The property values sets the JNDI com.sun.jndi.ldap.read.timeout property when attempting to establish a connection to a configured LDAP server. If the LDAP provider does not receive an LDAP response within the configured interval, it aborts the read attempt. The read timeout applies to the LDAP response from the server after the initial connection is established with the server. An integer value less than or equal to zero indicates no read timeout is specified.

Property	Default Value	Description
LDAPPoolMaxActive	8	Caps the number of concurrent LDAP connections to the LDAP server. A non-positive value indicates no limit. If this option is set for multiple LDAP providers, the value set by the first LDAP provider loaded takes precedence over all the others. When LDAPPoolMaxActive is reached, any further attempts by the LDAP provider classes to borrow LDAP connections from the pool are blocked indefinitely until a new or idle object becomes available in the pool. Connection pooling improves the LDAP provider's performance and resource utilization by managing the number of TCP connections established with configured LDAP servers.
controlFlag	optional	When you configure multiple authentication providers, use controlFlag for each provider to control how the authentication providers are used in the login sequence. controlFlag is a generic login module option rather than an LDAP configuration property.

Mapping Sybase Control Center Roles to LDAP or OS Groups

To grant Sybase Control Center privileges to users who are authenticated through LDAP or the operating system, associate roles used in Sybase Control Center with groups in LDAP or the operating system.

Prerequisites

- Required: Configure an LDAP authentication module.
- Optional: Create these LDAP groups and assign Sybase Control Center users to them:
 - sybase – confers sccUserRole. Assign all SCC users to the sybase group.
 - SCC Administrator – confers sccAdminRole. Assign only SCC administrators to this group.

Task

You can configure Sybase Control Center to enable users to authenticate through their local operating system or through an LDAP server. To make this type of authentication work, SCC roles must be mapped to groups that exist in the system providing authentication (LDAP or the operating system).

The sybase and SCC Administrator groups are convenient because they are predefined in `role-mapping.xml`. If you add sybase and SCC Administrator groups to your LDAP

Get Started

system and populate them with SCC users and administrators, you can skip to the next task—you do not need to complete the steps below.

The table lists default mappings of LDAP and OS groups to SCC roles. Login modules are defined in `csi_config.xml`.

Login Module	OS Group	Sybase Control Center Roles
UNIX Proxy	root	uaAnonymous, uaAgentAdmin, uaOSAdmin
	sybase	uaAnonymous, uaPluginAdmin, sccUserRole
	user	uaAnonymous
	guest	uaAnonymous
NT Proxy	Administrators	uaAnonymous, uaAgentAdmin, uaOSAdmin
	sybase	uaAnonymous, uaPluginAdmin, sccUserRole
	Users	uaAnonymous
	Guests	uaAnonymous
LDAP	sybase	uaAnonymous, uaPluginAdmin, sccUserRole
	SCC Administrator	uaAnonymous, sccAdminRole

There are two ways to accomplish the mapping:

- (Recommended) Add a “sybase” group and an “SCC Administrator” group to the operating system or LDAP server Sybase Control Center is using to authenticate users, and add all users who need to access Sybase Control Center to one or both groups.
- Configure Sybase Control Center to use existing groups in LDAP or the operating system by editing the `role-mapping.xml` file. This option is described here.

1. If Sybase Control Center is running, shut it down.

2. In a text editor, open:

```
<SCC-install-directory>/conf/role-mapping.xml
```

3. Locate the `sccUserRole` section of the file:

```
<Mapping>
  <LogicalName>sccUserRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
  <MappedName>SCC Agent Administrator</MappedName>
  <MappedName>sybase</MappedName>
</Mapping>
```

4. Add a `MappedName` line for the LDAP or OS group you are using to authenticate SCC users. The `sccUserRole` section should look similar to this:

```
<Mapping>
  <LogicalName>sccUserRole</LogicalName>
```



```

    <MappedName>SCC Administrator</MappedName>
    <MappedName>SCC Agent Administrator</MappedName>
    <MappedName>sybase</MappedName>
    <MappedName>my_SCC_group</MappedName>
  </Mapping>

```

5. Locate the sccAdminRole section of the file:

```

<Mapping>
  <LogicalName>sccAdminRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
</Mapping>

```

6. Add a MappedName line for the LDAP or OS group you are using to authenticate SCC administrators. The sccAdminRole section should look similar to this:

```

<Mapping>
  <LogicalName>sccAdminRole</LogicalName>
  <MappedName>SCC Administrator</MappedName>
  <MappedName>my_SCC_admin_group</MappedName>
</Mapping>

```

7. Save the file and exit.
8. (LDAP only) Ensure that the roles defined in the LDAP repository match the roles defined in role-mapping.xml.
9. In the <SCC-install-dir>\conf\csi_config.xml file, set the BindPassword and ProviderURL properties with values used in your deployment.
Sybase recommends that you encrypt sensitive values before saving them in csi_config.xml.
10. Start Sybase Control Center.

See also

- *Configuring an LDAP Authentication Module* on page 101
- *Configuring Authentication for Windows* on page 98
- *Configuring a Pluggable Authentication Module (PAM) for UNIX* on page 49
- *Assigning a Role to a Login or a Group* on page 119
- *User Authorization* on page 119

Encrypting a Password

Use the **passencrypt** utility to encrypt passwords and other values that must be kept secure while stored in text files.

You can safely store an encrypted password in a configuration file. Enter the password in clear text (unencrypted) when you execute **passencrypt** and when you use the password to log in.

passencrypt, which is located in the Sybase Control Center bin directory, uses the SHA-256 hash algorithm for passwords used in the PreConfiguredLoginModule in csi_config.xml.

Get Started

1. Open a command window and change to the `bin` directory:

Windows: `cd <SCC-install-directory>\bin`

UNIX: `cd <SCC-install-directory>/bin`

2. To encrypt a password, enter **passencrypt -csi**. Enter your new password at the resulting prompt.
passencrypt encrypts the password you enter (which does not appear on the screen) and displays the password in encrypted form.
3. Copy the encrypted password.
4. Paste the encrypted password where needed.

Configuring Ports

(Optional) Use the **scc --port** command to assign Sybase Control Center services to new ports.

Prerequisites

Check for port conflicts between Sybase Control Center and other software running on the same host.

Task

Sybase Control Center cannot function properly if other services use its ports. If you discover a conflict with any port listed in the right column below, you can either reconfigure the other service's port or reconfigure Sybase Control Center as described here.

Port Name	Description	Service Names	Property Names	Default Port
db	Database port Present on SCC server	SccSADataserver Messaging Alert Scheduler	com.sybase.asa.server.port messaging.db.port alert.database.port org.quartz.data-Source.ASA.URL	3638
http	Web HTTP port Present on SCC server	EmbeddedWebContainer	http.port	8282
https	Web HTTPS (secure HTTP) port Present on SCC server	EmbeddedWebContainer	https.port	8283

Port Name	Description	Service Names	Property Names	Default Port
jiniHttp	JINI HTTP server Present on SCC server and SCC agent	Jini	httpPort	9092
jiniRmid	JINI remote method invocation daemon Present on SCC server and SCC agent	Jini	rmiPort	9095
msg	Messaging port Present on SCC server	Messaging	messaging.port	2000
rmi	RMI port Present on SCC server and SCC agent	RMI	port	9999
tds	Tabular Data Stream™ port (used to communicate with other Sybase products) Present on SCC server and SCC agent	Tds	tdsPort	9998

1. Shut down Sybase Control Center.
2. Execute **scc --info ports** to display a list of Sybase Control Center services, their properties, and their assigned ports.
3. To reassign a port, enter a command in one of these formats:

```
scc --port port-name=port-number
```

```
scc --port service-name:property-name=port-number
```

Use the first, simpler format unless you want to configure the database services to use different ports. (By default, they all use the same port.)

4. Start Sybase Control Center.
5. Execute **scc --info ports** again to confirm that the port has been reassigned.

Examples

Set all four database services (data server, messaging, database alert, and scheduler) to the same port, 3639. (The database is SQL Anywhere®, used by the Sybase Control Center internal repository.)

```
scc --port db=3639
```

Get Started

Set only the database messaging service to port 3639.

```
scc --port Messaging:messaging.db.port=3639
```

Set the HTTP port to 9292.

```
scc --port http=9292
```

Set the Jini RMI daemon to port 9696.

```
scc --port jiniRmid=9696
```

Set the main Sybase Control Center messaging service to port 2001.

```
scc --port msg=2001
```

Set the RMI port to 9991.

```
scc --port rmi=9991
```

Set the Tabular Data Stream port to 9997.

```
scc --port tds=9997
```

Note: **scc** commands that include a port-setting option (**-p** or **--port**) do not start Sybase Control Center. To start SCC, execute a separate **scc** command.

See also

- *scc Command* on page 91

Configuring the E-mail Server

(Optional) Specify the e-mail server for Sybase Control Center to use to send e-mail alert notifications.

Prerequisites

Launch Sybase Control Center and log in using an account with administrative privileges. (The login account or its group must have `sccAdminRole`.)

Task

1. From the application's menu bar, select **Application > Administration**.
2. Select **General Settings**.
3. Click the **E-mail** tab.
4. Enter the name of the e-mail server through which Sybase Control Center will send alert notifications.
5. Change the default e-mail server port only in consultation with your e-mail administrator.

6. (Optional) Click **Customize e-mail settings** to display options for setting the domain name and e-mail sender for alert e-mail notifications.
 7. (Optional) Enter your domain name (for example, mycompany.com).
Most e-mail servers do not require SCC to provide an explicit domain name. Try providing a domain name here if your first attempt to configure e-mail alerts fails.
 8. (Optional) Change the default e-mail sender name.
This name appears in the "From" field of SCC e-mail alert messages. Do not use spaces; use hyphens or underscore characters instead.
-
- Tip:** If you have multiple SCC servers, configure their sender names so you can tell which SCC an alert is coming from. For example, SybaseControlCenter_Boston or SCC_test11.
-
9. (Optional) If you entered anything in the **E-mail Domain name** or **E-mail sender name** fields, click **Apply** to make the test e-mail option reappear.
 10. (Optional) To dispatch a test message, enter an e-mail address in the **Test e-mail address** field and click **Send**.
If the test e-mail is received, you have properly configured the server for e-mail alert notifications.
 11. Click **OK** (to apply the change and close the properties dialog) or **Apply** (to apply the change and leave the dialog open).

Next

(Optional) Configure automatic logout.

See also

- *Launching Sybase Control Center* on page 80
- *Logging in to Sybase Control Center* on page 95

Configuring the Automatic Logout Timer

(Optional) Set Sybase Control Center to end login sessions when users are inactive for too long.

Prerequisites

Launch Sybase Control Center and log in using an account with administrative privileges. (The login account or its group must have sccAdminRole.)

Task

1. From the application's menu bar, select **Application > Administration**.
2. Select **General Settings**.

3. Click the **Auto-Logout** tab.
4. Enter the number of minutes after which an idle user will be automatically logged out.
Enter 0 or leave the box empty to disable automatic logout.
5. Click **OK** (to apply the change and close the properties dialog) or **Apply** (to apply the change and leave the dialog open).

See also

- *Launching Sybase Control Center* on page 80
- *Logging in to Sybase Control Center* on page 95

Configuring Retrieval Thresholds for the Administration Console

(Optional) Set limits on the time the Administration Console waits for data to load or on the number of rows it loads.

Prerequisites

Launch Sybase Control Center and log in using an account with administrative privileges. (The login account or its group must have sccAdminRole.)

Task

Performing some tasks may cause the Administration Console to load a large amount of data, which can be time-consuming and can place a heavy load on your network. This is particularly likely if your perspective includes many resources. The Administration Console mitigates this problem by displaying partial results and by displaying placeholders called message rows when data takes longer than a specified number of seconds to retrieve or exceeds a specified number of rows. The data retrieval options let you specify those numbers.

This data retrieval scheme reduces network traffic because result sets that exceed the specified row count are not transmitted unless you ask for them by expanding a message row. By displaying partial results and message rows for data from slow-responding resources, the scheme also minimizes the time you spend waiting.

1. From the application's menu bar, select **Application > Administration**.
2. Select **General Settings**.
3. Click the **Administration Console** tab.
4. Set the timeout for data retrieval in seconds.

When SCC is not able to return all requested data within this period of time, it displays any data it has received and generates message rows in place of the missing results. The Administration Console replaces message rows with real data as soon as the data arrives.

5. Set the row count.

When a request returns results that exceed the specified row count, SCC displays a message row in place of the expected results. You can expand the message row by selecting it, clicking the drop-down arrow, and selecting **Expand**.

6. Click **OK** (to apply the change and close the properties dialog) or **Apply** (to apply the change and leave the dialog open).

See also

- *Searching and Filtering Resources* on page 322

User Authorization

The authorization mechanism in Sybase Control Center employs login accounts and task-based roles.

Access to Sybase Control Center is controlled by login accounts. You grant permissions to a login account by assigning predefined roles that control tasks the user can perform in Sybase Control Center, such as administration and monitoring of particular types of Sybase servers. The roles can be assigned directly to login accounts or to groups; a login account inherits the roles of any group to which it belongs. Component product modules assign some roles automatically.

Sybase Control Center classifies roles as follows:

- System roles – define how a user can interact with Sybase Control Center.
- Product roles – define how a user can interact with a particular managed resource in Sybase Control Center, for example the Replication Server named RepBoston01.

Note: The tools described here are for managing SCC-enabled login accounts; you cannot use them to manage accounts and groups that are native to your managed resource.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Assigning a Role to a Login or a Group

Use the security configuration options to add one or more roles to a Sybase Control Center login account or to a group. Roles enable users to perform tasks such as monitoring servers or administering Sybase Control Center.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task. To assign a monitoring role for a server, first register the server.

Task

Assign the sccAdminRole to any login account that will perform administrative tasks in Sybase Control Center.

1. From the application menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Click **Logins** or **Groups**.
4. In the table, select the login account or group to which you want to assign a role.
5. Click the **Roles** tab.
6. In the **Available roles for resource** list, select the role, then click **Add**. For example, to grant administrative privileges, add the SCC Service:sccAdminRole. To grant monitoring privileges, add the MonitorRole for the desired server and server type.

Note: Sybase Control Center product modules assign certain roles automatically, so you might not need to add a MonitorRole.

If a role appears in the **Has following roles** list, this account or group has already been configured with that role.

7. Click **OK**.

See also

- *Removing a Role from a Login or a Group* on page 120

Removing a Role from a Login or a Group

Use the security configuration options to remove one or more roles from a Sybase Control Center login account or from a group.

Prerequisites

You must have administrative privileges to perform this task.

Task

1. From the menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Click **Logins** or **Groups**.
4. Select the login account or group from which you want to remove a role.
5. Click the **Roles** tab.
6. Select the role, then click **Remove**.
7. Click **OK**.

See also

- *Assigning a Role to a Login or a Group* on page 119

Adding a Group

Use the security configuration options to create a new group.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

Groups can make roles easier to manage. Rather than assigning roles to individual users, assign roles to groups and add users to the groups or remove them as needed.

1. From the main menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Groups**.
4. Click **Create Group**.
5. Enter a group name and a description.
6. Click **Finish**.

See also

- *Removing a Group* on page 121
- *Adding a Login Account to a Group* on page 122
- *Removing a Login Account from a Group* on page 122

Removing a Group

Use the security configuration options to remove a group.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

1. From the main menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Groups**.
4. Select the group to remove.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.

See also

- *Adding a Group* on page 121
- *Adding a Login Account to a Group* on page 122
- *Removing a Login Account from a Group* on page 122

Adding a Login Account to a Group

Use the security configuration options to add one or more login accounts to a group.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

1. From the main menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Click **Groups**.
4. Select the group to which you want to assign an account.
5. Click the **Membership** tab.
6. Select the account, then click **Add**.
7. Click **OK**.

See also

- *Adding a Group* on page 121
- *Removing a Group* on page 121
- *Removing a Login Account from a Group* on page 122

Removing a Login Account from a Group

Use the security configuration options to remove one or more login accounts from a group.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

1. From the main menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties, expand the **Security** folder.
3. Select **Groups**.
4. Select the group from which to remove members.
5. Click the **Membership** tab.

6. Select the login, then click **Remove**.
7. Click **OK**.

See also

- *Adding a Group* on page 121
- *Removing a Group* on page 121
- *Adding a Login Account to a Group* on page 122

Adding a Login Account to the System

Use the security configuration options to create a native login account in Sybase Control Center.

Prerequisites

- You must have administrative privileges (sccAdminRole) to perform this task.
- If you intend to use LDAP or the operating system to authenticate users, configure the appropriate authentication module.

Task

Note: Sybase does not recommend that you manually create a native login account for every Sybase Control Center user. It is more efficient to configure Sybase Control Center to authenticate users through their user accounts in LDAP or the operating system. When you do that, SCC automatically creates a native account for every authenticated user.

1. From the main menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Logins**.
4. Click **Create Login**.
5. Enter a login name and expiration for the new account. Expiration is optional.
6. Click **Next**.
7. Select **Specify new user information**.
8. Enter details about the user:
 - Title
 - First name*
 - M.I. (middle initial)
 - Last name*
 - Suffix
 - E-mail address*
 - Phone

Get Started

- Ext.
- Fax
- Mobile
- Supports text messaging (checkbox)

*You must fill in the **First Name**, **Last Name**, and **E-mail Address** fields.

9. Click **Finish**.

Next

Grant privileges to the new login account. You can grant privileges by assigning Sybase Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping Sybase Control Center roles to the groups. The group approach is generally more efficient.

See also

- *Configuring Authentication for Windows* on page 98
- *Configuring a Pluggable Authentication Module (PAM) for UNIX* on page 49
- *Configuring an LDAP Authentication Module* on page 101
- *Removing a Login Account from the System* on page 124
- *Modifying a User Profile* on page 125

Removing a Login Account from the System

Use the security configuration options to delete a Sybase Control Center login account.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

1. From the main menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Logins**.
4. Select the login to delete.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.

See also

- *Adding a Login Account to the System* on page 123
- *Modifying a User Profile* on page 125

Modifying a User Profile

Use the security configuration options to suspend a login account, impose an expiration date, or modify the account's user information.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

1. From the main menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Logins**.
4. Select the login account to modify.
5. Click the **General** tab.
6. To suspend this account, click **Login disabled**.
7. To set the date on which this account will stop working, click the calendar icon next to the **Expiration** field and select a date.
8. Click **Apply**.
9. Click the **User Info** tab.
10. Edit the user information.
When this user configures e-mail alert subscriptions, Sybase Control Center automatically populates the subscription dialog with the e-mail address you enter here.
11. Click **Apply**.

See also

- *Adding a Login Account to the System* on page 123
- *Removing a Login Account from the System* on page 124

Logins, Roles, and Groups

Sybase Control Center includes predefined login accounts and roles.

A login account identifies a user who can connect to Sybase Control Center. An account has roles that control the tasks the user is allowed to perform. Users can be authenticated through native SCC accounts, but a safer approach is to delegate authentication to the operating system or to an LDAP directory service.

Sybase Control Center comes with a predefined login account. Sybase recommends using the predefined account only for installing and setting up Sybase Control Center. This account is not intended for use in a production environment.

Table 12. Predefined Login Account

Login Name	Description
sccadmin	Can use all the administration features in Sybase Control Center. Use for configuration and test.

A role is a predefined profile that can be assigned to a login account or a group. Roles control the access rights for login accounts. Sybase Control Center comes with predefined roles that are intended for use in production environments.

Table 13. Predefined Roles

Role	Description
sccUserRole	Provides nonadministrative access to Sybase Control Center. Required for all users and assigned automatically to every authenticated user.
sccAdminRole	Provides administrative privileges for managing Sybase Control Center.

Monitoring privileges for SCC product modules are assigned automatically.

A group is made up of one or more login accounts; all the accounts in a group have the roles granted to the group. In Sybase Control Center you can create groups to suit your business requirements.

Configure Sybase Control Center

Configure Sybase Control Center for SAP Sybase IQ.

Note: Before configuring Sybase Control Center for use in a production environment, complete the tasks in the *Get Started* section of the help. Setting up security is particularly important.

1. *Configuring SAP Sybase IQ Authority-Based Users for Monitoring*

For 15.3 and 15.4 databases, enable one or more SAP Sybase IQ authority-based users to authenticate an SAP Sybase IQ server with Sybase Control Center, create and populate the SCC_MONITOR group.

2. *Configuring SAP Sybase IQ Roles-Based Users for Monitoring*

For 16.0 and later databases, enable one or more SAP Sybase IQ role-based users or roles to authenticate an SAP Sybase IQ server with Sybase Control Center, create and populate the SCC_MONITOR role.

3. *Registering an SAP Sybase IQ Server*

Make Sybase Control Center aware of an SAP Sybase IQ resource (for example, a server that can be monitored) and its connection information by registering the resource.

4. *Configuring SAP Sybase IQ for Administration*

To perform administration tasks, you must have the correct authority or group membership (15.3 or 15.4) or system privileges and role membership (16.0), and you may need to register the server's Sybase Control Center agent.

5. *Importing Resources for Batch Registration*

(Optional) Import and register multiple servers from an interfaces or sql.ini file.

6. *Registering and Authenticating a Sybase Control Center Agent*

Register and authenticate the Sybase Control Center agent for a managed server.

7. *Creating a Perspective*

Create a perspective in which you can add and manage resources.

8. *Adding a Resource to a Perspective*

Add one or more resources to the current perspective.

9. *Authenticating a Login Account for a Managed Resource*

Specify the login account and password Sybase Control Center will use when it connects to your server or agent to collect monitoring data or manage the resource.

10. *Changing Update Frequency for Statistics and Charts*

You can control the rate at which data on monitor screens and charts is refreshed, the amount of time covered by charts, and the multiplex nodes included in charts.

11. *Setting Up Statistics Collection*

Use the Properties view of your managed resource to create a data collection job and add a schedule to the job.

12. *Creating an Alert*

Use the Add Alert wizard to create an alert instance for your resource.

13. *Key Performance Indicators for SAP Sybase IQ*

Key performance indicators (KPIs) provide the statistics that appear on SAP Sybase IQ screens and charts in Sybase Control Center.

14. *Optional Configuration Steps*

Perform additional configuration, including user authorization, alerts, data collection scheduling, backups, and setting purging options for the repository.

See also

- *User Authorization* on page 67
- *Logins, Roles, and Groups* on page 125
- *Setting Up Security* on page 96
- *Assigning a Role to a Login or a Group* on page 119

Configuring SAP Sybase IQ Authority-Based Users for Monitoring

For 15.3 and 15.4 databases, enable one or more SAP Sybase IQ authority-based users to authenticate an SAP Sybase IQ server with Sybase Control Center, create and populate the SCC_MONITOR group.

Prerequisites

Log in to SAP Sybase IQ as a user with DBA authority.

Task

To monitor a resource with SCC, you must authenticate the resource as an SAP Sybase IQ user with DBA authority or membership in the SCC_MONITOR group.

Note: If you are performing a quick start, you need only authenticate your resource with Sybase Control Center using an SAP Sybase IQ account with DBA authority (such as DBA). You can skip the steps below until you do a complete production set-up of SCC.

The SCC_MONITOR script must be executed for each managed resource.

1. Using Interactive SQL or another SQL command tool, execute **scc_iq_monitor_privileges_setup.sql**, located in the directory `SCC-3_2/plugins/IQMAP`.

The script creates the SCC_MONITOR group and grants a set of permissions.

2. Assign one or more SAP Sybase IQ users or groups to the SCC_MONITOR group. You can do this by either of these methods:
 - Using Interactive SQL or another SQL command tool, execute **grant membership in group SCC_MONITOR to <user/group>**
 - In a user interface tool such as Sybase Control Center, add the user to the SCC_MONITOR group

See also

- *Configuring SAP Sybase IQ Roles-Based Users for Monitoring* on page 129
- *Registering an SAP Sybase IQ Server* on page 130
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Feature Disabled on the Administration Console Task Menu* on page 1341
- *Authority-Based Users* on page 823

Configuring SAP Sybase IQ Roles-Based Users for Monitoring

For 16.0 and later databases, enable one or more SAP Sybase IQ role-based users or roles to authenticate an SAP Sybase IQ server with Sybase Control Center, create and populate the SCC_MONITOR role.

Prerequisites

- Requires the **MANAGE ROLES** and **MANAGE ANY OBJECT PRIVILEGE** system privileges to execute the SCC_MONITOR script, which populates the SCC_MONITOR role.
- Requires the **MANAGE ROLES** system privilege to grant the SCC_MONITOR role to any user or role.

Task

To monitor a resource with SCC, you must authenticate the resource as one of:

- A SAP Sybase IQ user or role granted the **MONITOR** system privilege (minimum system privileges to monitor).
- A member of the SCC_MONITOR role (maximum system privileges to monitor).

Note: If you are performing a quick start, you need only authenticate your resource with Sybase Control Center using the SAP Sybase IQ DBA user (granted maximum monitoring system privileges available) or an SAP Sybase IQ account granted **MONITOR** system privilege (the minimum system privilege required for monitoring). You can skip the steps below until you do a complete production set-up of SCC.

Configure Sybase Control Center

The SCC_MONITOR script must be executed for each managed resource.

1. Using Interactive SQL or another SQL command tool, execute **scc_iq_monitor_role_based_privileges_setup.sql**, located in the directory `SCC-3_2/plugins/IQMAP`.
The script creates the SCC_MONITOR role and grants a set of system privileges.
2. Assign one or more SAP Sybase IQ users or roles to the SCC_MONITOR role. You can do this by either of these methods:
 - Using Interactive SQL or another SQL command tool, execute **grant role SCC_MONITOR to <user/role>**
 - In a user interface tool such as Sybase Control Center, add the user or role to the SCC_MONITOR role

See also

- *Registering an SAP Sybase IQ Server* on page 130
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Feature Disabled on the Administration Console Task Menu* on page 1341
- *Role-Based Users* on page 892
- *Getting Started After Installing* on page 19
- *Configuring SAP Sybase IQ Authority-Based Users for Monitoring* on page 20

Registering an SAP Sybase IQ Server

Make Sybase Control Center aware of an SAP Sybase IQ resource (for example, a server that can be monitored) and its connection information by registering the resource.

Prerequisites

Ensure that the SAP Sybase IQ server does not have multiple databases. Sybase Control Center for SAP Sybase IQ supports a maximum of one database per server.

Task

1. In the Resource Explorer, select **Resources > Register**.
2. Specify:

Table 14. New Resource Type Details

Field	Description
Resource Name	(Required) Name of the resource to register. Enter the actual name of the server, including uppercase and lowercase letters. If the name registered in Sybase Control Center does not exactly match the server name, some monitoring functions may not work.
Resource Type	Select a resource type: <ul style="list-style-type: none"> • IQ Logical Server – register an SAP Sybase IQ logical server. • IQ Multiplex – register an SAP Sybase IQ multiplex server. • IQ Server – register an SAP Sybase IQ simplex server. Recommended. Can handle both simplex and multiplex servers.
Description	A brief description to help you identify the resource.

3. Click **Next**.
4. Specify the connection information for your resource:

Table 15. New Resource Connection Details

Field	Description
Host Name	(Required) Host name of the SAP Sybase IQ server.
IQ Port Number	(Required) Port number on server host.
Database	Name of the database.
Character Set	Character set to use for the connection.
Language	Language to use for the connection.
Logical Server	Name of the logical server. This only appears when registering a logical server.

5. (Optional) Enter a user name and password that SCC can use to authenticate with this resource to retrieve its software version. The credentials are used only for this purpose, then discarded.

If you prefer not to authenticate now, click **I do not want to supply authentication information**.

This step enables SCC to display the correct version information for the server before the server is formally authenticated (later in the configuration process).

6. Click **Next**.

7. (Optional) Click **Add this resource to the current perspective**. You must add a resource to a perspective (not necessarily the current perspective) before you can manage or monitor it.
8. (Optional) Click **Open the resource explorer to view this new resource**. (This option is not present when the Resource Explorer is open.)
The resource is added to the Resource Explorer even if you choose not to view it.
9. Click **Finish**.

See also

- *Common Display Options* on page 7
- *Resources* on page 1303
- *Unregistering a Resource* on page 1303

Configuring SAP Sybase IQ for Administration

To perform administration tasks, you must have the correct authority or group membership (15.3 or 15.4) or system privileges and role membership (16.0), and you may need to register the server's Sybase Control Center agent.

Prerequisites

- You have monitoring permissions
- The SAP Sybase IQ server you want to manage has a Sybase Control Center agent running on the same machine

Task

Before you can perform management tasks on an SAP Sybase IQ server, your login account must have the required permissions. To perform certain tasks, including starting and stopping the SAP Sybase IQ server, synchronizing the server, and adding secondary nodes, you must also register and authenticate the server's SCC agent.

1. Assign the authorities (15.3 or 16.4) or system privileges (16.0) required for administrative tasks to users who will perform those tasks. You can do this by granting the authorities or system privileges directly to user accounts or by granting the authorities or system privileges to a group or role and adding users to the group or role.
2. Register and authenticate the SCC agent associated with the SAP Sybase IQ server you want to manage.

Note: You must register the managed server before you can register its SCC agent.

See also

- *Importing Resources for Batch Registration* on page 277

Simplex Privilege Summary

A list of the system privileges and object permissions required to complete the various simplex server tasks

Editing the Simplex Server Configuration File

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Starting or Stopping a Simplex Server

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

Converting a Simplex Server to Multiplex

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Generating an Administration Script for a Simplex Server

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Simplex Server Properties

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	View any simplex property page – None required. Modify any simplex property – Requires DBA authority.
SAP Sybase IQ 16.0	View any simplex property page – None required. Modify any property on the Configuration or Options property page – Requires SERVER OPERATOR system privilege. Modify any property on the Request Logging property page – Requires one of: <ul style="list-style-type: none"> MANAGE PROFILING system privileges. SERVER OPERATOR system privileges.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Multiplex Privilege Summary

A list of the system privileges and object permissions required to complete the various multiplex server tasks

Editing the Multiplex Configuration File

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Starting or Stopping a Multiplex Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.

Database Version	Multiplex Privileges
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

Including a Secondary Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • All of these authorities: <ul style="list-style-type: none"> • MULTIPLEX ADMIN authority, and • BACKUP authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none"> • MANAGE MULTIPLEX system privilege. • SERVER OPERATOR system privilege. • BACKUP DATABASE system privilege.

Excluding a Secondary Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Synchronizing a Secondary Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires both SERVER OPERATOR and BACKUP DATABASE system privileges.

Adding a Secondary Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • All of these authorities: <ul style="list-style-type: none"> • MULTIPLEX ADMIN authority. • SPACE ADMIN authority. • BACKUP authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none"> • SERVER OPERATOR system privilege. • MANAGE MULTIPLEX system privilege. • MANAGE ANY DBSPACE system privilege. • BACKUP DATABASE system privilege.

Dropping a Secondary Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • All of these authorities: <ul style="list-style-type: none"> • MULTIPLEX ADMIN authority. • SPACE ADMIN authority. • BACKUP authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none"> • MANAGE MULTIPLEX system privilege.

Generating an Administration Script for Multiplex Nodes

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Converting a Simplex Server to Multiplex

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Reconfiguring a Multiplex Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Change server name, port or database location – Requires all of: <ul style="list-style-type: none"> • MULTIPLEX ADMIN authority. • BACKUP authority. All other changes require DBA authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none"> • SERVER OPERATOR system privilege. • BACKUP DATABASE system privilege.

Viewing or Modifying Multiplex Server Properties

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	View multiplex properties – None required. Modify multiplex properties – Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.

Database Version	Multiplex Privileges
SAP Sybase IQ 16.0	<p>View multiplex properties – None required.</p> <p>Modify any property on the Configuration – Requires all of:</p> <ul style="list-style-type: none"> • SERVER OPERATOR system privilege. • BACKUP DATABASE system privilege. • MANAGE MULTIPLEX system privilege. <p>Modify any property on the Options property page – Requires SERVER OPERATOR system privilege.</p> <p>Modify any property on the Request Logging property page – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE PROFILING system privileges. • SERVER OPERATOR system privileges.

Designating the Failover Node

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	<p>Requires all of:</p> <ul style="list-style-type: none"> • MANAGE MULTIPLEX system privilege. • SERVER OPERATOR system privilege. • BACKUP DATABASE system privilege.

Performing Coordinator Node Failover

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988

- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Logical Server Privilege Summary

A list of the system privileges and object permissions required to complete the various logical server tasks

Creating a Logical Server

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Deleting a Logical Server

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Configuring Logical Server Node Membership

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Altering a Logical Server Assignment

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Generating DDL Commands for a Logical Server

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Logical Server Properties

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	View logical server properties – None required. Modify logical server properties – Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	View any logical server property page – None required. Modify any logical server property – Requires MANAGE MULTIPLEX system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Logical Server Policy Privilege Summary

A list of the system privileges and object permissions required to complete the various logical server policy tasks

Creating a Logical Server Policy

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Deleting a Logical Server Policy

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Generating DDL Commands for a Logical Server Policy

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Logical Server Policy Properties

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	View any logical server policy property page – None required. Modify any logical server policy property – Requires MANAGE MULTIPLEX system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988

- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Remote Server Privilege Summary

A list of the system privileges and object permissions required to complete the various remote server tasks

Creating a Remote Server

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

Testing a Remote Server Connection

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Deleting a Remote Server

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

Generating Remote Server DDL Commands

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Remote Server Properties

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	View remote server properties – None required. Modify remote server properties – Requires DBA authority.
SAP Sybase IQ 16.0	View any remote server property page – None required. Modify any remote server property – Requires SERVER OPERATOR system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

External Login Privilege Summary

A list of the system privileges and object permissions required to complete the various external login tasks

Creating an External Login

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Deleting an External Login

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.

Database Version	External Login Privileges
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Generating External Login DDL Commands

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing External Login Properties

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Database Privilege Summary

A list of the system privileges and object permissions required to complete the various database tasks.

Creating a Database

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	Required DBA authority. The account under which the server is running must have write permissions on the directories where files are created.
SAP Sybase IQ 16.0	The account under which the server is running must have write permissions on the directories where files are created. No other system privilege is required.

Creating a Database Using CSV File

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	The account under which the server is running must have write permissions on the directories where files are created. No other system privilege is required.

Setting Database Options

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	View database options only – None required. Modify database options – Requires DBA authority.
SAP Sybase IQ 16.0	View database options only – None required. Modify database options – Depending on the option being modified, requires one of: <ul style="list-style-type: none"> • SET ANY PUBLIC OPTION system privilege. • SET ANY SECURITY OPTION system privilege. • SET ANY SYSTEM OPTION system privilege.

Viewing or Modifying Database Properties

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	View database license management property page – Requires EXECUTE permission on the sp_iqlmconfig system procedure to display content of page. View any other database property page – None required. Modify the following properties on the Settings page requires: <ul style="list-style-type: none"> • Include SQL statement information option – Requires EXECUTE permission on the sa_server_option system procedure to modify this setting. • Collect Information about deadlocks option – Requires DBA authority. • Clear Deadlock Information Now option – Requires DBA authority. Modify any other database property – Requires DBA authority.

Database Version	Database Privileges
SAP Sybase IQ 16.0	<p>View database license management property page –</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sp_iqlm-config system procedure to display content of page. • If the system procedure security model* of the selected database is set to Invoker, you require the SERVER OPERATOR system privilege to display content of page. <p>View any other database property page – None required.</p> <p>Modify the following properties on the Settings page requires:</p> <ul style="list-style-type: none"> • Refresh button – Requires SERVER OPERATOR or ALTER DATABASE system privilege. • Collect Information about deadlocks option – Requires SET ANY SYSTEM OPTION system privilege. • Include SQL statement information option – <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_server_option system procedure to modify this setting. • If the system procedure security model* of the selected database is set to Invoker, you require the SERVER OPERATOR system privilege to display content of page. • Clear Deadlock Information Now option – Requires SERVER OPERATOR system privilege. <p>Modify properties on the license management page –</p> <ul style="list-style-type: none"> • Requires SERVER OPERATOR system privilege. <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Table Privilege Summary

A list of the system privileges and object permissions required to complete the various table tasks.

Creating a Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Base table to be owned by self:</p> <ul style="list-style-type: none"> Requires RESOURCE authority with CREATE permission on the main store dbspace in which the table is created. <p>Base table to be owned by any user – Requires DBA authority.</p>
SAP Sybase IQ 16.0	<p>Base table to be owned by self –</p> <ul style="list-style-type: none"> Requires CREATE permission on the dbspace where the table is created. Also requires one of: <ul style="list-style-type: none"> CREATE TABLE system privilege. CREATE ANY OBJECT system privilege <p>Base table to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE permission on the dbspace where the table is created. Also requires one of: <ul style="list-style-type: none"> CREATE ANY TABLE system privilege. CREATE ANY OBJECT system privilege

Creating a Global Temporary Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Global temporary table to be owned by self:</p> <ul style="list-style-type: none"> Requires RESOURCE authority with CREATE permission on the main store dbspace in which the table is created. <p>Global temporary table to be owned by any user – Requires DBA authority.</p>

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>Global temporary table to be owned by self:</p> <ul style="list-style-type: none"> Requires CREATE TABLE system privilege. <p>Global temporary table to be owned by any user – Requires one of:</p> <ul style="list-style-type: none"> CREATE ANY TABLE system privilege. CREATE ANY OBJECT system privilege.

Creating a Proxy Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Proxy table to be owned by self:</p> <ul style="list-style-type: none"> Requires RESOURCE authority with CREATE permission on the main store dbspace in which the table is created. <p>Proxy table to be owned by any user – Requires DBA authority.</p>
SAP Sybase IQ 16.0	<p>Proxy table to be owned by self – Requires CREATE PROXY TABLE system privilege.</p> <p>Proxy table to be owned by any user – Requires one of:</p> <ul style="list-style-type: none"> CREATE ANY TABLE system privilege CREATE ANY OBJECT system privilege.

Viewing Table Data in the Execute SQL Windows

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of the following to enable menu option:</p> <ul style="list-style-type: none"> DBA authority. SELECT permission on the table. You own the table. <p>Queries execute with user's current permissions.</p>
SAP Sybase IQ 16.0	<p>Requires one of the following to enable menu option:</p> <ul style="list-style-type: none"> SELECT ANY TABLE system privilege. SELECT permission on the table. You own the table. <p>Queries execute with user's current privileges.</p>

Deleting a Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY TABLE system privilege. • DROP ANY OBJECT system privilege. • You own the table.

Generating Table DDL Commands

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Moving a Table to Another Dbspace

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority. • You own the table and have CREATE permission on the target dbspace.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • ALTER permission on the table and CREATE permission on the target dbspace. • You own the table and have CREATE permission on the target dbspace.

Validating a System Store Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • VALIDATE authority.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

Setting the Primary Key

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER and REFERENCE permission on the table. • You own the table.
SAP Sybase IQ 16.0	To create a new or modify an existing primary key - Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace where the table resides. • ALTER and REFERENCE permission on the table. • You own the table. <p>To modify the name only of an existing primary key, requires ALTER ANY INDEX system privilege.</p>

Setting a Clustered Index

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table.

Database Version	Table Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • ALTER and REFERENCE permission on the table. • You own the table.

Moving Table Data from RLV Store to IQ Main Store

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege.

Calculating the Number of Rows in a Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. • You own the table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table.

Moving Table Objects to Another Dbspace

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires CREATE permission on the target dbspace.</p> <p>Also requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the table. • You own the table.
SAP Sybase IQ 16.0	<p>Requires CREATE permission on the target dbspace.</p> <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • Requires MANAGE ANY DBSPACE system privilege. • You own the table.

Enabling Row-Level Versioning in a Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege.

Viewing or Modifying Base Table Properties

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any property page of a base table owned by self – None required.</p> <p>View any property page of a base table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. • You own the table. <p>Modify any property on the General page requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table. <p>Modify any property on the Miscellaneous page requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603 • <i>Table Trigger Privilege Summary</i> on page 615 • <i>Table Partition Privilege Summary</i> on page 639

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>View any property page of a base table owned by self – None required.</p> <p>View any property page of a base table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify the table name on the General page – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • You own the table. <p>Use the Calculate button on the Miscellaneous page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify any other property on the Miscellaneous page for an IQ catalog (system) store table – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table. • You own the table. <p>Modify a comment on the General page – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege • ALTER ANY TABLE system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603 • <i>Table Trigger Privilege Summary</i> on page 615

Database Version	Table Privileges
	<ul style="list-style-type: none"> • <i>Table Partition Privilege Summary</i> on page 639

Viewing or Modifying Global Temporary Table Properties

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any property page of a global temporary table owned by self – None required.</p> <p>View any property page of a global temporary table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. • You own the table. <p>Modify any property on the General page requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table. <p>Modify any property on the Miscellaneous page requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603 • <i>Table Trigger Privilege Summary</i> on page 615

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>View any property page of a global temporary table owned by self – None required.</p> <p>View any property page of a global temporary table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify the table name on the General page – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • You own the table. <p>Use the Calculate button on the Miscellaneous page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify any other property on the Miscellaneous page for an IQ catalog (system) store table – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table. • You own the table. <p>Modify a comment on the General page – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege • ALTER ANY TABLE system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603

Database Version	Table Privileges
	<ul style="list-style-type: none"> • <i>Table Trigger Privilege Summary</i> on page 615

Viewing or Modifying Proxy Table Properties

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any property page of a proxy table owned by self – None required except for Data page, which requires SELECT permission on the base table on the remote server.</p> <p>View any properties of a proxy table owned by any user – None required except for Data page, which requires:</p> <ul style="list-style-type: none"> • SELECT permission on the base table on the remote server. • Also requires one of: <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. <p>Modify any property on the General or Miscellaneous page requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Trigger Privilege Summary</i> on page 615

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>View any property page of a proxy table owned by self – None required except for Data page, which requires SELECT permission on the base table on the remote server.</p> <p>View any property page of a proxy table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the proxy table. • SELECT permission on the base table. • You own the table. <p>Use the Calculate button on the Miscellaneous page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the proxy table. • You own the table. <p>Modify a comment on the General page requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Trigger Privilege Summary</i> on page 615

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Table Column Privilege Summary

A list of the system privileges and object permissions required to complete the various table column tasks.

Adding a Column

Database Version	Table Column Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Create a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER permission on the table. • You own the underlying table. <p>Create a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER and REFERENCE permission on the table. • You own the underlying table.
SAP Sybase IQ 16.0	<p>Create a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of the following: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the underlying table. <p>Create a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of the following: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • Both ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

Deleting a Column

Database Version	Table Column Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Deleting a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER permission on the table. • You own the underlying table. <p>Deleting a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER and REFERENCE permission on the table. • You own the underlying table.
SAP Sybase IQ 16.0	<p>Deleting a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the underlying table. • You own the underlying table. <p>Deleting a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • Both ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

Viewing or Modify Column Properties

Database Version	Table Column Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any table column property page – None required.</p> <p>Modify the Primary key property on the General page – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER and REFERENCE permission on the table. • You own the table. <p>Modify any other table column property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table.
SAP Sybase IQ 16.0	<p>View any table column property page – None required.</p> <p>Modify the Primary key property on the General page – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • Both ALTER and REFERENCE permission on the table. • You own the table. <p>Modify a table column comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>Modify any other table column property – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table. • You own the table.

See also

- *Adding a System Privilege to a Role-Based User* on page 902

- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Table Permissions Privilege Summary

A list of the system privileges and object permissions required to complete the various table permission tasks.

Grant and Revoke Permissions on a Table

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You have administrative rights (with grant option) to the permission.• You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You have administrative rights (with grant option) to the permission.• You own the database object.

Adjust Administration Permissions on a Table

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You have administrative rights to the permission being modified.• You own the database object.

See also

- *Adding a System Privilege to a Role-Based User* on page 902

- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Table Constraints Privilege Summary

A list of the system privileges and object permissions required to complete the various table constraints tasks.

Creating a Column Check Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • You have ALTER permission on the underlying table. • You own the underlying table.

Creating a Foreign Key Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • Requires one of: <ul style="list-style-type: none"> • ALTER permission on the derived table • You own the derived table. • Also requires one of: <ul style="list-style-type: none"> • REFERENCE permission on the base table. • You own the base table. • Also requires one of: <ul style="list-style-type: none"> • REFERENCE permission on the derived table (to index it) • You own the derived table.

Database Version	Table Constraint Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> ALTER ANY OBJECT system privilege. CREATE permission on the dbspace the table is defined on, along with one of: <ul style="list-style-type: none"> ALTER ANY TABLE system privilege. ALTER permission on the derived table. You own the derived table. <p>Also requires one of:</p> <ul style="list-style-type: none"> CREATE ANY INDEX system privilege. CREATE ANY OBJECT system privilege. REFERENCE permission on the base table.

Creating a Table Check Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> DBA authority. ALTER permission on the underlying table. You own the underlying table.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> ALTER ANY OBJECT system privilege. ALTER ANY TABLE system privilege. You have ALTER permission on the underlying table. You own the underlying table.

Creating a Unique Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> DBA authority. ALTER and REFERENCE permission on the underlying table. You own the underlying table.

Database Version	Table Constraint Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace the table is defined on, along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

Deleting a Table or Column Check Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the underlying table.

Deleting a Unique, Primary or Foreign Key Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

Rebuilding a Unique, Primary or Foreign Key Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY INDEX system privilege. • REFERENCE permission on the underlying table. • You own the underlying table.

Validating a Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • VALIDATE authority.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

Generating Constraint DDL Commands

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Constraint Properties

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View table constraint properties – None required.</p> <p>Modify comment on foreign key or unique constraint – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• ALTER permission on the underlying table.• You own the underlying table.

Database Version	Table Constraint Privileges
SAP Sybase IQ 16.0	<p>View any table constraint property page – None required.</p> <p>Modify the comment on a foreign or primary key constraint – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>Modify the comment on a unique key constraint – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • ALTER ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>Modify the definition of a table or column check constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table. <p>Modify any foreign key constraint property on the Action page – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE ANY INDEX system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the table. <p>Modify any other property of a primary, foreign or unique key, table check or column check constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege.

Database Version	Table Constraint Privileges
	<ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the underlying table.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Table Index Privilege Summary

A list of the system privileges and object permissions required to complete the various index tasks on tables.

Creating a Table Index

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires CREATE permission on the specified dbspace. Also requires one of: <ul style="list-style-type: none"> • DBA authority • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	Requires CREATE permission on the specified dbspace. Also requires one of: <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

Deleting a Table Index

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY INDEX system privilege. • DROP ANY OBJECT system privilege. • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

Rebuilding a Table Index

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

Validating a Table Index

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	Require VALIDATE ANY OBJECT system privilege.

Moving a Table Index

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority. • CREATE permission on the target dbspace, along with one of: <ul style="list-style-type: none"> • You own the underlying table. • You have REFERENCE permission on the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • You own the underlying table of the index. • Reference permission on the table along with one of: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the target dbspace.

Generating Index DDL Commands

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Index Properties

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View table index fragmentation property page – Requires EXECUTE permission on the sp_iqindexfragmentation system procedure to display content of page.</p> <p>View any other table index property page – None required.</p> <p>Modify any index property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

Database Version	Table Index Privileges
SAP Sybase IQ 16.0	<p>View table index fragmentation property page –</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sp_iqindexfragmentation system procedure to display content of page. • If the system procedure security model* of the selected database is set to Invoker, you require the MANAGE ANY DBSPACE system privilege to display content of page. <p>*The system procedure security model of the selected database appears on the General page of database properties.</p> <p>View any other table index property page – None required.</p> <p>Modify a table index comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • ALTER ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the underlying table of the index. <hr/> <p>Note: ALTER permission on the table is not required to modify the comment only.</p> <hr/> <p>Modify any other table index property –</p> <ul style="list-style-type: none"> • Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY INDEX system privilege, • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Table Trigger Privilege Summary

A list of the system privileges and object permissions required to complete the various table trigger tasks on database objects.

Creating a Table Trigger

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority, along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege. • CREATE ANY OBJECT system privilege. <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.

Deleting a Table Trigger

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority, along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • You own the underlying table of the trigger.

Generating Table Trigger DDL Commands

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Table Trigger Properties

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any trigger property page – None required.</p> <p>Modify any trigger property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority, along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.
SAP Sybase IQ 16.0	<p>View any trigger property page – None required.</p> <p>Modify a trigger comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege • ALTER ANY TRIGGER system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege <hr/> <p>Note: ALTER permission on the table is not required to modify a comment.</p> <hr/> <p>Modify any other trigger property:</p> <ul style="list-style-type: none"> • Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TRIGGER system privilege, along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • You own the underlying table of the trigger.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941

- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Table Partition Privilege Summary

A list of the system privileges and object permissions required to complete the various table partition tasks.

Creating a Hash Partition

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.
SAP Sybase IQ 16.0	<p>Requires one of the following:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table.

Creating a Range Partition

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • CREATE permission on the dbspaces where the partitions are being created. <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER permission on the table. • You own the table.

Database Version	Table Partition Privileges
SAP Sybase IQ 16.0	<p>Requires one of the following:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspaces along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table.

Creating a Hash-Range Partition

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority, and one of: <ul style="list-style-type: none"> • ALTER permission on the table. • You own the table.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table.

Deleting a Partition

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.

Database Version	Table Partition Privileges
SAP Sybase IQ 16.0	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

Unpartitioning a Table

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.
SAP Sybase IQ 16.0	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

Merging Partitions

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.
SAP Sybase IQ 16.0	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

Splitting Partitions

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • SELECT permission on the table.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on table. <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table.

Moving Partitions

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority • CREATE permission on the dbspace to which the partition is being moved along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the table.

Database Version	Table Partition Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • One of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace to which the partition is being moved. • Along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the underlying table.

Managing Column Storage in a Table Partition

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority • CREATE permission on the dbspace to which the partition is being moved along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.

Database Version	Table Partition Privileges
SAP Sybase IQ 16.0	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • One of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace to which the partition is being moved. • Along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the underlying table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

Viewing or Modifying Table Partition Properties

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority • CREATE permission on the dbspace to which the partition is being moved along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.

Database Version	Table Partition Privileges
SAP Sybase IQ 16.0	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • One of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace to which the partition is being moved. • Along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the underlying table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

View Privilege Summary

A list of the system privileges and object permissions required to complete the various view tasks.

Creating a View

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority • RESOURCE authority with SELECT permission on the tables in the view definition to create a view owned by you.
SAP Sybase IQ 16.0	View to be owned by self – <ul style="list-style-type: none"> • Requires CREATE VIEW system privilege. • Also requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT object permission on the underlying tables of the view. View to be owned by any user – Requires one of: <ul style="list-style-type: none"> • CREATE ANY VIEW system privilege. • CREATE ANY OBJECT system privilege. • Also requires one of: <ul style="list-style-type: none"> • SELECT object permission on the underlying tables of the view. • SELECT ANY TABLE system privilege.

Viewing View Data in the Execute SQL Window

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	None required. Query executes with user's current permissions.
SAP Sybase IQ 16.0	None required. Query executes with user's current permissions.

Recompiling and Enabling a View

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • All of these: <ul style="list-style-type: none"> • SELECT permission on the underlying tables of the view. • You own the view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the view. • Also require one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the underlying tables of the view.

Disabling a View

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the view.

Deleting a View

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the view.

Database Version	View Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY VIEW system privilege. • DROP ANY OBJECT system privilege. • You own the view.

Generating View DDL Commands

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying View Properties

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any view property page – None required.</p> <p>Modify view permissions – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object. <p>Modify any other view property except those relating to triggers – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the view. <p>For privileges relating to triggers, see:</p> <ul style="list-style-type: none"> • <i>View Trigger Privilege Summary</i> on page 685

Database Version	View Privileges
SAP Sybase IQ 16.0	<p>View any view property page – None required.</p> <p>Modify view permissions – Requires one of:</p> <ul style="list-style-type: none"> • <code>MANAGE ANY OBJECT PRIVILEGE</code> system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object. <p>Modify a view comment – Requires any one of:</p> <ul style="list-style-type: none"> • <code>CREATE ANY VIEW</code> system privilege. • <code>CREATE ANY OBJECT</code> system privilege. • <code>ALTER ANY VIEW</code> system privilege. • <code>ALTER ANY OBJECT</code> system privilege. • <code>COMMENT ANY OBJECT</code> system privilege. • You own the view. <p>Modify any other view property, except those relating to triggers – Requires one of:</p> <ul style="list-style-type: none"> • <code>ALTER ANY VIEW</code> system privilege. • <code>ALTER ANY OBJECT</code> system privilege. • You own the view. <p>For privileges relating to view triggers, see:</p> <ul style="list-style-type: none"> • <i>View Trigger Privilege Summary</i> on page 685

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

View Permissions Privilege Summary

A list of the system privileges and object permissions required to complete the various view permission tasks.

Grant and Revoke Permissions on a View

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object.
SAP Sybase IQ	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

Adjust Administration Permissions on a View

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839

- *Adding an Authority to a Group* on page 859

View Trigger Privilege Summary

A list of the system privileges and object permissions required to complete the various view trigger tasks on database objects.

Creating a View Trigger

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority and you own the underlying view of the trigger.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege. • CREATE ANY OBJECT system privilege. Also requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY VIEW system privilege. • You own the underlying view of the trigger.

Deleting a View Trigger

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the underlying view of the trigger.
SAP Sybase IQ 16.0	Requires ALTER permission on the underlying view of the trigger by virtue of any one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY VIEW system privilege. • You own the underlying view of the trigger.

Generating View Trigger DDL Commands

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying View Trigger Properties

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View trigger properties only – None required.</p> <p>Modify trigger comment or properties – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority and you own the underlying view of the trigger.
SAP Sybase IQ 16.0	<p>View any trigger property page – None required.</p> <p>Modify a trigger comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege • ALTER ANY TRIGGER system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege <hr/> <p>Note: ALTER permission on the view is not required to modify a comment.</p> <hr/> <p>Modify any other trigger property:</p> <ul style="list-style-type: none"> • Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TRIGGER system privilege, along with one of: <ul style="list-style-type: none"> • ALTER ANY VIEW system privilege. • You own the underlying view of the trigger.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988

- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Materialized View Privilege Summary

A list of the system privileges and object permissions required to complete the various materialized view tasks.

Creating a Materialized View

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Materialized view to be owned by self –</p> <ul style="list-style-type: none"> • Requires RESOURCE authority with SELECT permission on tables in the view definition. • Requires CREATE permission on the selected dbspace to create a view owned by you. <p>Materialized view to be owned by any user – Requires DBA authority.</p>
SAP Sybase IQ 16.0	<p>Materialized view to be owned by self –</p> <ul style="list-style-type: none"> • Requires CREATE MATERIALIZED VIEW system privilege. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE object permission on the dbspace where the materialized view is being created. • Also requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT object permission on the underlying tables of the materialized view. <p>Materialized view to be owned by any user –</p> <ul style="list-style-type: none"> • Requires CREATE object permission on the dbspace where the materialized view is being created. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY MATERIALIZED VIEW system privilege. • CREATE ANY OBJECT system privilege. • And also requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT object permission on the underlying tables of the materialized view.

Viewing Materialized View Data in the Execute SQL Window

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	None required. Query executes with user's current permissions.
SAP Sybase IQ 16.0	None required. Query executes with user's current permissions.

Truncating Materialized View Data

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the materialized view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • TRUNCATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • TRUNCATE permission on the materialized view. • You own the materialized view.

Validating Materialized View Data

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the materialized view.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

Refreshing Materialized View Data

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires DBA authority.</p> <p>Also requires both of:</p> <ul style="list-style-type: none"> • INSERT permission on the underlying tables of the materialized view or you own the materialized view. • SELECT permission on the underlying tables of the materialized view or you own the underlying tables of the materialized view.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • INSERT ANY TABLE system privilege. • INSERT permission on the materialized view. • You own the materialized view. <p>Also requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the underlying tables of the materialized view. • You own the underlying tables of the materialized view.

Recompiling and Enabling Materialized View Data

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the materialized view and have one of the following: <ul style="list-style-type: none"> • SELECT permission on the underlying tables of the materialized view. • You own the underlying tables of the view.

Database Version	Materialized View Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view. <p>Also requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the underlying tables of the materialized view. • You own the underlying tables of the materialized view.

Disabling Materialized View Data

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the materialized view.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view.

Deleting a Materialized View

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY MATERIALIZED VIEW system privilege. • DROP ANY OBJECT system privilege. • You own the materialized view.

Generating Materialized View DDL Commands

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Setting a Clustered Index on a Materialized View

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• You own the materialized view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• ALTER ANY MATERIALIZED VIEW system privilege.• ALTER ANY OBJECT system privilege.• You own the materialized view.

Viewing or Modifying Materialized View Properties

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any materialized view property page – None required.</p> <p>Modify materialized view permissions – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object. <p>Modify the SQL page of the materialized view properties – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the materialized view and have SELECT permission on the underlying tables. <p>Modify any other materialized view property except those relating to indexes – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying tables. • SELECT permission on the underlying tables. • You own the materialized view. <p>For privileges relating to materialized view indexes, see:</p> <ul style="list-style-type: none"> • <i>Materialized View Index Privilege Summary</i> on page 743

Database Version	Materialized View Privileges
SAP Sybase IQ 16.0	<p>View any materialized view property page – None required.</p> <p>Modify materialized view permissions – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object. <p>Modify a materialized view comment – Requires any one of:</p> <ul style="list-style-type: none"> • CREATE ANY MATERIALIZED VIEW system privilege • ALTER ANY MATERIALIZED VIEW system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege • You own the materialized view. <p>Modify the SQL page of the materialized view properties – Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY MATERIALIZED VIEW system privilege. • DROP ANY OBJECT system privilege. • You own the materialized view. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY MATERIALIZED VIEW system privilege. • CREATE ANY OBJECT system privilege. <p>Modify any other materialized view property except those relating to indexes – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view. <p>For privileges relating to materialized view indexes, see:</p> <ul style="list-style-type: none"> • <i>Materialized View Index Privilege Summary</i> on page 743

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049

- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Materialized View Permissions Privilege Summary

A list of the system privileges and object permissions required to complete the various materialized view permission tasks.

Grant and Revoke Permissions on a Materialized View

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• Administrative rights over the permission.• You own the database object.
SAP Sybase IQ	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You have administrative rights (with grant option) to the permission.• You own the database object.

Adjust Administration Permissions on a Materialized View

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You have administrative rights to the permission being modified.• You own the database object.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988

- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Materialized View Index Privilege Summary

A list of the system privileges and object permissions required to complete the various index tasks materialized views.

Creating a Materialized View Index

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority • You own the underlying database object of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace, along with one of: <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • You own the materialized view index.

Deleting a Materialized View Index

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the underlying database object of the index. • You own the underlying database object of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY INDEX system privilege. • DROP ANY OBJECT system privilege. • You own the materialized index.

Rebuilding a Materialized View Index

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the underlying database object of the index. • You own the underlying database object of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • You own the underlying database object of the index.

Validating a Materialized View Index

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • VALIDATE authority.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

Generating Materialized View Index DDL Commands

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Materialized View Index Properties

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any materialized view index property page – None required.</p> <p>Modify any materialized view index property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the underlying database object of the index. • You own the underlying database object of the index.
SAP Sybase IQ 16.0	<p>View any materialized view index property page – None required.</p> <p>Modify a materialized view index comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • ALTER ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. <hr/> <p>Note: ALTER permission on the materialized view is not required to modify the comment only.</p> <hr/> <p>Modify any other materialized view index property – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace, along with one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • You own the materialized view.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Domain Privilege Summary

A list of the system privileges and object permissions required to complete the various domain tasks.

Creating a Domain

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • CREATE DATATYPE system privilege. • CREATE ANY OBJECT system privilege.

Deleting a Domain

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP DATATYPE system privilege. • DROP ANY OBJECT system privilege. • You own the domain.

Generating Domain DDL Commands

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing Domain Properties

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Text Configuration Privilege Summary

A list of the system privileges and object permissions required to complete the various text configuration tasks.

Creating a Text Configuration Object

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Text configuration object to be owned by self – Requires RESOURCE authority. Text configuration object to be owned by any user – Requires DBA authority.
SAP Sybase IQ 16.0	Text configuration object to be owned by self – Requires CREATE TEXT CONFIGURATION system privilege. Text configuration object to be owned by any user – Requires one of: <ul style="list-style-type: none"> • CREATE ANY TEXT CONFIGURATION system privilege. • CREATE ANY OBJECT system privilege. Also requires one of: <ul style="list-style-type: none"> • ALTER ANY TEXT CONFIGURATION system privilege. • ALTER ANY OBJECT system privilege.

Deleting a Text Configuration Object

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Text configuration object owned by self – None required. Table configuration object owned by any user – Requires DBA authority.
SAP Sybase IQ 16.0	Text configuration object owned by self – None required. Table configuration object owned by any user – Requires one of: <ul style="list-style-type: none"> • DROP ANY TEXT CONFIGURATION system privilege. • DROP ANY OBJECT system privilege.

Generating Text Configuration Object DDL Commands

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Text Configuration Object Properties

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	View any text object configuration property page – None required. Modify any text object configuration property – Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the text configuration object.

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 16.0	<p>View any text object configuration property page – None required.</p> <p>Modify a text configuration object term breaker or external prefilter property – Requires:</p> <ul style="list-style-type: none"> • CREATE ANY EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY TEXT CONFIGURATION system privilege. • ALTER ANY OBJECT system privilege. • You own the text configuration object. <p>Modify a text configuration object comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TEXT CONFIGURATION system privilege. • ALTER ANY TEXT CONFIGURATION system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the text configuration. <p>Modify any other text configuration object properties – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TEXT CONFIGURATION system privilege. • ALTER ANY OBJECT system privilege. • You own the text configuration object.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Text Index Privilege Summary

A list of the system privileges and object permissions required to complete the various text index tasks.

Creating a Text Index

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table being indexed along with CREATE permission on the dbspace where the index is being created. • You own the underlying table being indexed along with CREATE permission on the dbspace where the index is being created. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege along with CREATE permission on the dbspace where the index is being created. • CREATE ANY OBJECT system privilege. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

Deleting a Text Index

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY INDEX system privilege. • DROP ANY OBJECT system privilege. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

Refreshing a Text Index

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

Truncating a Text Index

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table being indexed. • You own the underlying table being indexed. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table being indexed. • You own the underlying table being indexed. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

Generating Text Index DDL Commands

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	None required to generate DDL commands; however, requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.

Database Version	Text Index Privileges
SAP Sybase IQ 16.0	<p>None required to generate DDL commands; however,</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

Viewing or Modifying Text Index Properties

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p> <p>View text index properties – None required.</p> <p>Rename a text index – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table. • You own the underlying table being indexed. <p>Move a text index – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority. • You own the underlying table being indexed and have CREATE permission on the target dbspace. <p>Modify comment on a text index – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the underlying table being indexed.

Database Version	Text Index Privileges
SAP Sybase IQ 16.0	<p>Requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p> <p>View any text index property page – None required.</p> <p>Rename a text index – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • REFERENCE permission on the underlying table. • You own the underlying table being indexed. <p>Move a text index – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE • One of the following: <ul style="list-style-type: none"> • You own the underlying table being indexed. • REFERENCE permission on the table along with one of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the target dbspace. <p>Modify a text index comment – Requires:</p> <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege. • Also requires one of:

Database Version	Text Index Privileges
	<ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • CREATE ANY OBJECT system privilege. • CREATE ANY INDEX system privilege. • COMMENT ANY OBJECT system privilege. • You own the underlying table being indexed.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Sequence Generator Privilege Summary

A list of the system privileges and object permissions required to complete the various sequence generator tasks.

Creating a Sequence Generator

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • CREATE ANY SEQUENCE system privilege. • CREATE ANY OBJECT system privilege.

Deleting a Sequence Generator

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY SEQUENCE system privilege. • DROP ANY OBJECT system privilege. • You own the sequence generator.

Restarting a Sequence at Start Value

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY SEQUENCE system privilege. • ALTER ANY OBJECT system privilege. • You own the sequence generator.

Generating Sequence Generator DDL Commands

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Sequence Generator Properties

Database Version	Sequence Generator Permissions
SAP Sybase IQ 15.3 and 15.4	<p>View sequence generator properties – None required.</p> <p>Modify a sequence comment – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority. • You own the sequence generator. <p>Modify sequence permissions – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the sequence generator. <p>Modify any other sequence property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the sequence generator.
SAP Sybase IQ 16.0	<p>View any sequence property page – None required.</p> <p>Modify a sequence comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY SEQUENCE system privilege. • ALTER ANY SEQUENCE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. <p>Modify sequence permissions – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the sequence generator. <p>Modify any other sequence property – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY SEQUENCE system privilege. • ALTER ANY OBJECT system privilege. • You own the sequence generator.

Granting and Revoking Sequence Generator USAGE Permission

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the sequence generator.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Spatial Support Privilege Summary

A list of the system privileges and object permissions required to complete the various spatial support tasks.

Creating a Spatial Reference System

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • CREATE ANY OBJECT system privilege.

Deleting a Spatial Reference System

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • DROP ANY OBJECT system privilege.

Generating Spatial Reference System DDL Commands

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Spatial Reference System Properties

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	View spatial reference system properties – None required. Modify spatial reference system properties or comments – Requires one of: <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 16.0	<p>View spatial reference system properties – None required.</p> <p>Modify spatial reference system properties – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • ALTER ANY OBJECT system privilege. <p>Modify spatial reference system comment – Requires one of:</p> <ul style="list-style-type: none"> • COMMENT ANY OBJECT system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY SPATIAL OBJECT system privilege.

Creating a Spatial Unit of Measure

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • MANAGE ANY SPATIAL OBJECT.

Deleting a Spatial Unit of Measure

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • DROP ANY OBJECT system privilege.

Generating Spatial Unit of Measure DDL Commands

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Spatial Unit of Measure Properties

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View spatial unit of measure properties – None required.</p> <p>Modify spatial unit of measure properties or comments – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	<p>View any spatial unit of measure property page – None required.</p> <p>Modify a spatial unit of measure comment – Requires one of:</p> <ul style="list-style-type: none"> • COMMENT ANY OBJECT system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY SPATIAL OBJECT system privilege. <p>Modify any other spatial unit of measure property – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • ALTER ANY OBJECT system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Authority-Based User Privilege Summary

A list of the system privileges and object permissions required to complete the various authority-based user tasks.

Creating an Authority-Based User

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • Both USER ADMIN and PERMS ADMIN authorities.
SAP Sybase IQ 16.0	Not supported.

Deleting an Authority-Based User

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Converting an Authority-Based User to a Group

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Viewing or Modifying Authority-Based User Options

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Not supported.

Generating Authority-Based User DDL Commands

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	Not supported.

Viewing or Modifying Authority-Based User Properties

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	<p>View any user property page – None required.</p> <p>Modify a password – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. • PERMS ADMIN authority. <p>Modify a login policy – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. <p>Modify any other user property except those relating to permissions –</p> <ul style="list-style-type: none"> • Requires DBA authority. <p>For privileges relating to user permissions, see:</p> <ul style="list-style-type: none"> • <i>Authority-Based Database Object Permissions Privilege Summary</i> on page 889
SAP Sybase IQ 16.0	Not Supported.

Changing an Authority-Based User Password

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

Forcing an Authority-Based User Password Change

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

Unlocking an Locked Authority-Based User Account

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

Changing an Authority-Based User Login Policy

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

Granting or Revoking an Authority from a User

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941

- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Authority-Based Group Privilege Summary

A list of the system privileges and object permissions required to complete the various authority-based group tasks.

Creating an Authority-Based Group

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • Both USER ADMIN and PERMS ADMIN authorities
SAP Sybase IQ 16.0	Not supported.

Deleting an Authority-Based Group

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Converting an Authority-Based Group to a User

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Adding Authority-Based Users and Groups to Groups

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Removing Authority-Based Users and Groups from a Group

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Viewing or Modifying Authority-Based Group Options

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Generating Authority-Based Group DDL Commands

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	Not supported.

Viewing or Modifying Authority-Based Group Properties

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	<p>View any property page – None required.</p> <p>Modify a password – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. • PERMS ADMIN authority. <p>Modify a login policy – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. <p>Modify any other group property except those relating to permissions –</p> <ul style="list-style-type: none"> • Requires DBA authority. <p>For privileges relating to group permissions, see:</p> <ul style="list-style-type: none"> • <i>Authority-Based Database Object Permissions Privilege Summary</i> on page 889
SAP Sybase IQ 16.0	Not supported

Granting or Revoking an Authority to a Group

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Authority-Based Database Object Permissions Privilege Summary

A list of the system privileges and object permissions required to complete the various authority-based user and group tasks pertaining to database objects.

Grant or Revoke Permissions on a Table or Column

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You have administrative rights (with grant option) to the permission. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

Modify Administrative Permissions on a Table or Column

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

Grant or Revoke Permissions on a View or Materialized View

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

Modify Administrative Permissions on a View or Materialized View

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

Grant or Revoke Permissions on a Sequence Generator

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Not supported.

Grant or Revoke Permissions on a Function or Procedure

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

Grant or Revoke Permissions on a Dbspace

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Role-Based User Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based user tasks.

Creating a Role-Based User

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Creating a user requires MANAGE ANY USER system privilege.</p> <p>Granting a role during the user creation process requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the role being granted (role administrator). • MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>Granting a system privilege during user creation requires administrative rights over the system privilege being granted.</p>

Deleting a Role-Based User

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Converting a Role-Based User to a User Extended Role

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege.

Adding and Removing a User from a Role

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

Adding and Removing System Privileges from a User

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege.

Viewing or Modifying Role-Based User Options

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.

Database Version	Role-Based User Privileges
SAP Sybase IQ 16.0	<p>View the list of options – None required.</p> <p>Modify any option – Depending on the option being modified, requires one of these:</p> <ul style="list-style-type: none"> • SET ANY PUBLIC OPTION system privilege. • SET ANY SECURITY OPTION system privilege. • SET ANY SYSTEM OPTION system privilege.

Generating Role-Based User DDL Commands

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Role-Based User Properties

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	<p>View any user property page – None required.</p> <p>Modify a password – Requires CHANGE PASSWORD system privilege.</p> <p>Modify a login policy, comment, or refresh DN – Requires MANAGE ANY USER system privilege.</p> <p>Refresh LDAP DN - Requires MANAGE ANY USER system privilege.</p> <p>For privileges relating to user permissions, see:</p> <ul style="list-style-type: none"> • <i>Role-Based Database Object Permissions Privilege Summary</i> on page 1034

Changing a Role-Based User Password

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.

Database Version	Role-Based User Privileges
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Forcing a Role-Based User Password Change

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires CHANGE PASSWORD system privilege.

Unlocking a Role-Based User Account

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Changing a Role-Based User Login Policy

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Role-Based User-Extended Role Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based user-extended role tasks.

Creating a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Creating a role requires both the MANAGE ANY USER and MANAGE ROLES system privileges.</p> <p>Granting a role during user-extended role creation requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the role being granted (role administrator). • MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>Granting a system privilege during user-extended role creation requires administrative rights over the system privilege being granted.</p>

Deleting a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Converting a User-Extended Role to a Role-Based User

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the role being converted.

Adding and Removing Grantees to and from a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

Changing Administrative Rights of a Grantee of a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

Adding and Removing Underlying Roles to and from a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Changing Administrative Rights on an Underlying Role of a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Adding and Removing System Privileges to and from a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

Changing Administrative Rights on a System Privileges Granted to a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

Viewing or Modifying User-Extended Role Options

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	<p>View user-extended role options only – None required.</p> <p>Modify user-extended role options – Depending on the option being modified, requires one of these:</p> <ul style="list-style-type: none"> • SET ANY PUBLIC OPTION system privilege. • SET ANY SECURITY OPTION system privilege. • SET ANY SYSTEM OPTION system privilege.

Managing Role Administrators of a User-Extended Role

Database Version	Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the role being managed. • MANAGE ROLES system privilege if the role being granted has a global role administrator.

Adding the Global Role Administrator to a User-Extended Role

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the role being managed.

Removing the Global Role Administrator from a User-Extended Role

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role being managed. MANAGE ROLES system privilege.

Generating User-Extended Role DDL Commands

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying User-Extended Role Properties

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	<p>View any user-extended role property page – None required.</p> <p>Modify a password – Requires CHANGE PASSWORD system privilege.</p> <p>Modify a login policy, or refresh LDAP DN – Requires MANAGE ANY USER system privilege.</p> <p>Modify a user-extended role comment – Requires one of:</p> <ul style="list-style-type: none"> MANAGE ROLES system privilege. Administrative rights over the role begin commented. <p>For privileges relating to user-extended role permissions, see:</p> <ul style="list-style-type: none"> <i>Role-Based Database Object Permissions Privilege Summary</i> on page 1034

Changing a User-Extended Role Password

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires CHANGE PASSWORD system privilege.

Forcing a User-Extended Role Password Change

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Unlocking a User-Extended Role Account

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Changing a User-Extended Role Login Policy

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Role-Based Standalone Role Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based standalone role tasks.

Creating a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 16.0	<p>Creating a role requires <code>MANAGE ROLES</code> system privilege.</p> <p>Granting a role during standalone role creation requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role being granted (role administrator). <code>MANAGE ROLES</code> system privilege if the role being granted has a global role administrator. <p>Granting a system privilege during standalone creation requires administrative rights over the system privilege being granted.</p>

Deleting a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role being deleted. <code>MANAGE ROLES</code> system privilege if the role being deleted has a global role administrator.

Adding and Removing Grantees to and from a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). <code>MANAGE ROLES</code> system privilege if the role has a global role administrator.

Changing a Grantee's Administrative Rights on a User-Extended Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

Adding and Removing Underlying Roles to and from a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Changing Administrative Rights on an Underlying Role of a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Adding and Removing System Privileges to and from a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

Changing Administrative Rights on a System Privileges Granted to a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

Managing Role Administrators of a Standalone Role

Database Version	Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role Administrator Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role being managed. MANAGE ROLES system privilege if the role being granted has a global role administrator.

Adding the Global Role Administrator to a Standalone Role

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the role being managed.

Removing the Global Role Administrator from a Standalone Role

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role being managed. MANAGE ROLES system privilege.

Generating Standalone Role DDL Commands

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying User-Extended Role Properties

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 16.0	<p>View any standalone role property page – None required.</p> <p>Modify a standalone role comment – Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role being commented. MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>For privileges relating to standalone role permissions, see:</p> <ul style="list-style-type: none"> <i>Role-Based Database Object Permissions Privilege Summary</i> on page 1034

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Role-Based Database Object Permissions Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based user, user-extended role, or standalone role tasks relating to database objects.

Grant or Revoke Permissions on a Table or Column

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You have administrative rights (with grant option) to the permission. You own the database object.

Modify Administrative Permissions on a Table or Column

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You have administrative rights to the permission being modified. You own the database object.

Grant or Revoke Permissions on a View or Materialized View

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You have administrative rights (with grant option) to the permission. You own the database object.

Modify Administrative Permissions on a View or Materialized View

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You have administrative rights to the permission being modified. You own the database object.

Grant or Revoke Permissions on a Function or Procedure

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You own the database object.

Grant or Revoke Permissions on a Sequence Generator

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You own the sequence generator.

Grant or Revoke Permissions on a Dbspace

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Role-Based System Role Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based system role tasks.

View Grantees, Underlying Roles, and System Privileges Granted to a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Adding and Removing Grantees to and from a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege.

Adding and Removing Underlying Roles to and from a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires the MANAGE ROLES system privilege.</p> <p>To then add an underlying role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Changing Administrative Rights of an Underlying Role on a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires the MANAGE ROLES system privilege.</p> <p>To then add an underlying role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Adding and Removing System Privileges from a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege along with administrative rights over the system privilege.

Changing Administrative Rights of an Underlying Role on a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege along with administrative rights over the system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Role-Based Compatibility Role Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based compatibility role tasks.

View Grantees, Underlying Roles, and System Privileges Granted to a Compatibility Role

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Granting and Revoking a Grantee to and from a Compatibility Roles

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the compatibility role.

Deleting Compatibility Roles

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the compatibility role being deleted.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Role-Based System Privilege Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based system privilege tasks.

View Users and Roles Granted to a System Privilege

Database Version	Role-Based System Privilege Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Adding and Removing Grantees to and From a System Privilege

Database Version	Role-Based System Privilege Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over any system privilege.

Changing Administrative Rights of a Grantee of a System Privilege

Database Version	Role-Based System Privilege Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over any system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Login Mapping Privilege Summary

A list of the system privileges and object permissions required to complete the various login mapping tasks.

Creating a Login Mapping

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority along with SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege along with one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view.

Deleting a Login Mapping

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority along with SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege along with one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view.

Generating Login Mapping DDL Commands

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	Requires SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view.

Viewing Login Mapping Properties

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View Login Mapping properties – Requires SELECT permission on the SYSLOGINMAP view.</p> <p>Modify Login Mapping comment – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority along with SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	<p>View any login mapping property page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view. <p>Modify a login mapping comment –</p> <ul style="list-style-type: none"> • Requires MANAGE ANY USER system privilege along with one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Login Policy Privilege Summary

A list of the system privileges and object permissions required to complete the various login policy tasks.

Creating a Login Policy for a Simplex or Multiplex

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY LOGIN POLICY system privilege.

Deleting a Login Policy

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY LOGIN POLICY system privilege.

Generating Login Policy DDL Commands

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing Login Policy Properties

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	View any login policy property page – None required. Modify any login policy property – Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.

Database Version	Login Policy Privileges
SAP Sybase IQ 16.0	View any login policy property page – None required. Modify any login policy property – Requires MANAGE ANY LOGIN POLICY system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

LDAP Server Configuration Object Privilege Summary

A list of the system privileges and object permissions required to complete the various LDAP server configuration object tasks for SAP Sybase IQ.

Creating an LDAP Server Configuration Object

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

Deleting an LDAP Server Configuration Object

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

Activating, Suspending, and Refreshing an LDAP Server Configuration Object

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

Validating User

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

Generating LDAP Server Configuration Object DDL Commands

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying LDAP Server Configuration Object Properties

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	View any LDAP server property page – None Required. Modify any LDAP server property – Requires MANAGE ANY LDAP SERVER system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Dbospace Privilege Summary

A list of the system privileges and object permissions required to complete the various dbospace tasks.

Creating a Dbspacespace

Database Version	Dbospace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Deleting a Dbspacespace

Database Version	Dbospace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Preallocating Space for a Dbspacespace

Database Version	Dbospace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Generating Dbspacespace DDL Commands

Database Version	Dbospace Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Changing a Dbspace to Read-Only

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Viewing or Modifying Dbspace Properties

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	View any dbspace property page – None required. Modify dbspace permissions – Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. Modify any other dbspace property – Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	View any dbspace property page – None required. Modify dbspace permissions – Requires MANAGE ANY DBSPACE system privilege. Modify any other dbspace property – Requires MANAGE ANY DBSPACE system privilege.

Granting and Revoking Dbspace CREATE Permission

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941

Configure Sybase Control Center

- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

DB File Privilege Summary

A list of the system privileges and object permissions required to complete the various DB file tasks.

Creating a DB File

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Deleting a DB File

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Emptying a DB File

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Generating DB File DDL Commands

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying DB File Properties

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	View any db file property page – None required. Modify any db file property – Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	View any db file property page – None required. Modify any db file property – Requires MANAGE ANY DBSPACE system privilege.

Granting or Revoking Dbspace CREATE Permission

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Event Privilege Summary

A list of the system privileges and object permissions required to complete the various event tasks.

Creating an Event

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. CREATE ANY OBJECT system privilege.

Deleting an Event

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. DROP ANY OBJECT system privilege.

Disabling or Enabling an Event

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. ALTER ANY OBJECT system privilege.

Triggering an Event

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.

Database Version	Event Privileges
SAP Sybase IQ 16.0	Requires MANAGE ANY EVENT system privilege.

Generating Event DDL Commands

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Event Properties

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	View event properties – None required. Modify event comment or properties – Requires DBA authority.
SAP Sybase IQ 16.0	View event properties only – None required. Modify event properties – Requires one of: <ul style="list-style-type: none"> • MANAGE ANY EVENT system privilege. • ALTER ANY OBJECT system privilege. Modify event comment only – Requires one of: <ul style="list-style-type: none"> • MANAGE ANY EVENT system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege

Creating an Event Schedule

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY EVENT system privilege. • ALTER ANY OBJECT system privilege.

Deleting an Event Schedule

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. ALTER ANY OBJECT system privilege.

Generating Event Schedule DDL Commands

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Event Schedule

Properties

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	View any event schedule property page – None required. Modify any event schedule property – Requires DBA authority.
SAP Sybase IQ 16.0	View any event schedule property page – None required. Modify any event schedule property – Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. ALTER ANY OBJECT system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Java External Environment Privilege Summary

A list of the system privileges and object permissions required to complete the various external environment java tasks.

Installing a Java Classes or JAR File

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Updating a Java Classes or JAR File

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Deleting a Java Classes or JAR File

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Viewing or Modifying a Java Classes or JAR File

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	View external environment properties – None required. Modify external environment properties – Requires DBA authority.
SAP Sybase IQ 16.0	View external environment properties – None required. Modify external environment properties – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Testing the Configuration of a Java External Environment

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL ENVIRONMENT system privilege.

Viewing or Modifying Java External Environment Properties

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL ENVIRONMENT system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Perl External Environment Privilege Summary

A list of the system privileges and object permissions required to complete the various Perl external environment tasks.

Installing a Perl Object

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Updating a Perl Object

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Deleting a Perl Object

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Viewing or Modifying a Perl Object Properties

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	View external environment properties – None required. Modify View external environment properties – Requires DBA authority.
SAP Sybase IQ 16.0	View external environment properties – None required. Modify external environment properties – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Testing the Configuration of a Perl External Environment

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Viewing or Modifying Perl External Environment Properties

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

PHP External Environment Privilege Summary

A list of the system privileges and object permissions required to complete the various PHP external environment tasks.

Installing a PHP Object

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	View external environment properties – None required. Modify external environment properties – Requires DBA authority.
SAP Sybase IQ 16.0	View external environment properties – None required. Modify external environment properties – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Updating a PHP Object

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Deleting a PHP Object

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Viewing or Modifying a PHP Object Properties

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	View properties – None required. Modify comment – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Testing the Configuration of a PHP External Environment

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Viewing or Modifying PHP External Environment Properties

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page– None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839

- *Adding an Authority to a Group* on page 859

Other External Environment Privilege Summary

A list of the system privileges and object permissions required to complete the various external environment tasks.

Viewing or Modifying C ESQL, C ODBC, or CLR (.NET) Executable Properties

Database Version	Other External Environment Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Function Privilege Summary

A list of the system privileges and object permissions required to complete the various function tasks.

Creating a Watcom SQL or Transact-SQL Function

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	Watcom SQL or Transact-SQL function to be owned by self – Requires one of: <ul style="list-style-type: none">• DBA authority.• RESOURCE ADMIN authority. Watcom SQL or Transact-SQL function to be owned by any user – <ul style="list-style-type: none">• Requires DBA authority.

Database Version	Function Privileges
SAP Sybase IQ 16.0	<p>Watcom SQL or Transact-SQL to be owned by self –</p> <ul style="list-style-type: none"> Requires CREATE PROCEDURE system privilege. <p>Watcom SQ or Transact-SQL function to be owned by any user –</p> <p>Requires one of:</p> <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege.

Creating an External C/C++ Scalar or Aggregate Function

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>External C/C++ Scalar or Aggregate function to be owned by self or any user –</p> <ul style="list-style-type: none"> Requires DBA authority.
SAP Sybase IQ 16.0	<p>External C/C++ Scalar or Aggregate function to be owned by self –</p> <p>Requires all of:</p> <ul style="list-style-type: none"> CREATE PROCEDURE system privilege. CREATE EXTERNAL REFERENCE system privilege. <p>External C/C++ Scalar or Aggregate function to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE EXTERNAL REFERENCE system privilege. Also requires one of: <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege.

Creating an External Java Function

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>External Java function to be owned by self or any user – Requires DBA authority.</p>

Database Version	Function Privileges
SAP Sybase IQ 16.0	<p>External Java function to be owned by self –</p> <p>Requires all of:</p> <ul style="list-style-type: none"> • CREATE PROCEDURE system privilege. • CREATE EXTERNAL REFERENCE system privilege. <p>External Java function to be owned by any user –</p> <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege.

Deleting a Function

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the function.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY PROCEDURE system privilege. • DROP ANY OBJECT system privilege. • You own the function.

Generating Function DDL Commands

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Function Properties

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any function property page regardless of type – None required.</p> <p>Modify permissions for any function type – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object. <p>Modify any other function property regardless of type – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• You own the function.

Database Version	Function Privileges
SAP Sybase IQ 16.0	<p>View any function property page regardless of type – None required.</p> <p>Modify SQL code for Watcom SQL or Transact-SQL function – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the function. <p>Modify SQL code for External C/C++ Scalar or Aggregate, or External Java function – Requires one of:</p> <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the function. <p>Modify a comment for any function type – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • ALTER ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the function. <p>Modify permissions for any function type – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the database object.

Granting or Revoking Function EXECUTE Permission

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.

Database Version	Database Object Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You own the database object.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Procedure Privilege Summary

A list of the system privileges and object permissions required to complete the various procedure tasks.

Creating a Procedure

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Watcom SQL or Transact-SQL procedure to be owned by self – Requires one of:</p> <ul style="list-style-type: none"> DBA authority. RESOURCE ADMIN authority. <p>Watcom SQL or Transact-SQL, to be owned by any user –</p> <ul style="list-style-type: none"> Requires DBA authority. <p>External C/C++ or External Environment procedure to be owned by self or any user – Requires one of:</p> <ul style="list-style-type: none"> DBA authority.

Database Version	Procedure Privileges
SAP Sybase IQ 16.0	<p>Watcom SQL or Transact-SQL procedure to be owned by self –</p> <ul style="list-style-type: none"> Requires CREATE PROCEDURE system privilege. <p>Watcom SQL or Transact-SQL procedure to be owned by any user – Requires one of:</p> <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege <p>External C/C++ or External Environment procedure to be owned by self – Requires all of:</p> <ul style="list-style-type: none"> CREATE EXTERNAL REFERENCE system privilege. CREATE PROCEDURE system privilege. <p>External C/C++ or External Environment procedure to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE EXTERNAL REFERENCE system privilege. Also requires one of: <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege

Creating a Remote Procedure

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Remote procedure to be owned by self or any user –</p> <ul style="list-style-type: none"> Requires DBA authority.
SAP Sybase IQ 16.0	<p>Remote procedure to be owned by self –</p> <ul style="list-style-type: none"> Requires CREATE PROCEDURE system privilege. <p>Remote procedure to be owned by any user –</p> <ul style="list-style-type: none"> Requires one of: <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege.

Creating a Table UDF or TPF

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	<p>Table UDF or TPF to be owned by self –</p> <ul style="list-style-type: none"> Requires all of: <ul style="list-style-type: none"> CREATE EXTERNAL REFERENCE system privilege. CREATE PROCEDURE system privilege. <p>Table UDF or TPF to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE EXTERNAL REFERENCE system privilege. Also requires one of: <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege.

Executing a Procedure Using View Data in SQL

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> DBA authority. You have EXECUTE permission on the procedure. You own the procedure.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> EXECUTE ANY PROCEDURE system privilege. You have EXECUTE permission on the procedure. You own the procedure

Deleting a Procedure

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> DBA authority. You own the procedure.

Database Version	Procedure Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY PROCEDURE system privilege. • DROP ANY OBJECT system privilege. • You own the procedure.

Generating Procedure DDL Commands

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Procedure Properties

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any procedure property page regardless of type – None required.</p> <p>Modify permissions for any procedure type – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object. <p>Modify any other procedure property regardless of type – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the procedure.

Database Version	Procedure Privileges
SAP Sybase IQ 16.0	<p>View any procedure property page regardless of type – None required.</p> <p>Modify SQL code for Watcom-SQL or Transcat-SQL procedures – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the procedure. <p>Modify SQL code for Table UDFs, TPFs, or External Environment procedures –</p> <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the procedure. <p>Modify a comment for any procedure type – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • ALTER ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the procedure. <p>Modify permissions for any procedure type – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the database object.

Granting or Revoking Procedure EXECUTE Permission

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.

Database Version	Database Object Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You own the database object.

See also

- Adding a System Privilege to a Role-Based User* on page 902
- Adding a System Privilege to a User-Extended Role* on page 941
- Adding a System Privilege to a Standalone Role* on page 988
- Adding a System Privilege to a System Role* on page 1049
- Adding an Authority to an Authority-Based User* on page 839
- Adding an Authority to a Group* on page 859

Web Service Privilege Summary

A list of the system privileges and object permissions required to complete the various Web service tasks.

Creating a Web Service

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY WEB SERVICE system privilege.

Enabling or Disabling a Web Service

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY WEB SERVICE system privilege.

Deleting a Web Service

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY WEB SERVICE system privilege.

Generating Web Service DDL Commands

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Web Service Properties

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	View any Web service property page – None required. Modify any Web service property – Requires DBA authority.
SAP Sybase IQ 16.0	View any Web service property page – None required. Modify any Web service property – Requires MANAGE ANY WEB SERVICE system privilege.

See also

- *Adding a System Privilege to a Role-Based User* on page 902
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Adding a System Privilege to a Standalone Role* on page 988
- *Adding a System Privilege to a System Role* on page 1049
- *Adding an Authority to an Authority-Based User* on page 839
- *Adding an Authority to a Group* on page 859

Importing Resources for Batch Registration

(Optional) Import and register multiple servers from an `interfaces` or `sql.ini` file.

Prerequisites

Copy the `interfaces` or `sql.ini` file to a location on or accessible from the machine that hosts your Web browser.

Task

An `interfaces` (UNIX) or `sql.ini` file (Windows) is a list of Sybase servers and their ports; it may contain other connection information as well. The file is created during the installation of a Sybase server:

Configure Sybase Control Center

- Windows: %SYBASE%\ini\sql.ini
- Unix: \$SYBASE/interfaces

For more information on `interfaces` files, see the appendix on configuration files in *Configuration Guide Open Client and Open Server 15.0 for UNIX*.

For more information on `sql.ini` files, see the chapter on network communications using `sql.ini` in the Adaptive Server Enterprise 15.0 *Configuration Guide for Windows*.

Note: The Import Resources wizard imports servers in batches of a single type (Adaptive Server, SAP Sybase IQ, or Replication Server, for example). If your `interfaces` or `sql.ini` file includes resources of more than one type, you must perform this procedure for each resource type.

1. In the application menu, select **View > Open > Resource Explorer**.
2. In the Resource Explorer, select **Resources > Import**.
The Import Resources wizard opens; **Interfaces file** is already selected.
3. Click **Next**.
The Directory Service Connection page appears.
4. Click **Browse** and navigate to the `interfaces` file you want to import from.
You cannot type in the **File name** field.
5. Click **Next**.
6. On the Import Resource Type page, select the type of server you want to import.
7. On the Resource Selection page, click to select the servers you want to import.
Select only servers of the type you chose on the Import Resource Type page. If you import servers with incorrect types, Sybase Control Center will not be able to monitor or manage them properly.
8. Resources of your chosen type may require connection parameters in addition to those present in the file—RSSD host name and port for Replication Server, for example, or character set and language for Adaptive Server. Enter any required connection parameters.
9. Click **Next**.
10. (Optional) Click **Add these resources to the current perspective**. You must add a resource to a perspective (not necessarily the current perspective) before you can manage or monitor it.
11. Click **Next**.
The Confirmation page displays a list of the resources you have selected.
12. Click **Finish** if you are ready to import, or click **Back** to return to the previous screens and change your selections.
When you click **Finish**, Sybase Control Center imports and registers the resources and displays a summary page.
13. Click **Close** to finish the wizard.

The newly imported resources appear in the Resource Explorer. If you elected to add them to the current perspective, the resources also appear in the Perspective Resources view.

See also

- *Configuring SAP Sybase IQ for Administration* on page 132
- *Resources* on page 1303
- *Unregistering a Resource* on page 1303

Registering and Authenticating a Sybase Control Center Agent

Register and authenticate the Sybase Control Center agent for a managed server.

The Sybase Control Center agent runs on a managed server and enables Sybase Control Center to manage it. The SCC agent is installed automatically as part of the Sybase server.

To perform certain administrative tasks, including starting and stopping a Sybase IQ server, syncing the server, and adding secondary nodes, you must register and authenticate the server's SCC agent.

1. In the Perspective Resources view, select a resource.
2. From the application menu bar, select **View > Open > Administration Console**.
3. In the left pane of the Administration Console, select either:
 - **IQ Servers**
 - **IQ Servers > Multiplex Management > Multiplex Servers**
4. Select **Resource > Register Agent**.
5. Enter the IQ server host name and agent port (the default port is 9999) and click **OK**.
6. In the Administration Console, select the same IQ server or multiplex server and select **Resource > Authenticate Agent**.
7. Depending on your database version, do one of the following:
 - For 15.x - Enter the Sybase Control Center agent user (the default is uafadmin) and password (by default, there is no password—leave the field blank).
 - For 16.0 - Enter the Sybase Control Center agent user (the default is uafadmin) and password (created during the installation process).

Next

For instructions on changing the password for the SCC agent's default uafadmin account, see the topic on setting passwords in the *Sybase Control Center Installation Guide*.

See also

- *Creating a Perspective* on page 281

Viewing Sybase Control Center Agent Connection Information

View Sybase Control Center agent connection information in the server properties.

1. In the Perspective Resources view, select a resource.
2. From the application menu bar, select **View > Open > Administration Console**.
3. In the left pane of the Administration Console, select either:
 - **IQ Servers**
 - **IQ Servers > Multiplex Management > Multiplex Servers**
4. Select the server or multiplex node from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. Select **Agent** from the left pane.

Area	Description
Agent Page	<p>Agent registered – Indicates if the Sybase Control Center agent is registered: true or false.</p> <p>Agent authenticated – Indicates if the Sybase Control Center agent is authenticated: true or false.</p> <p>Agent status – Status of the Sybase Control Center agent: Running, Stopped, or Unknown.</p> <p>Agent host – Name of the host machine where the Sybase Control Center agent is running.</p> <p>Agent port – Port number on the host machine where the Sybase Control Center agent is running.</p> <p>Agent user – User name for authentication of the agent. Default is <i>uafadmin</i>.</p> <p>Agent process owner – The user name that owns the agent process.</p> <p>Agent home – The home directory of the Sybase Control Center agent.</p> <p>Agent version – The version of the Sybase Control Center agent.</p> <p>SCC agent plugin version – The agent plugin version of the Sybase Control Center agent.</p> <p>IQ directory – Installation directory of the IQ server with which the Sybase Control Center agent is associated.</p> <p>IQ version – Version of the IQ server with which the Sybase Control Center agent is associated.</p>

Creating a Perspective

Create a perspective in which you can add and manage resources.

1. From the application menu bar, select **Perspective > Create**.
2. Enter a name for your perspective. The name can contain up to 255 characters.
3. Click **OK**.

See also

- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Perspectives* on page 1306

Adding a Resource to a Perspective

Add one or more resources to the current perspective.

Prerequisites

Register the resources.

Task

Add servers or other resources to a perspective so you can monitor and manage them along with other resources in the same perspective.

1. From the Sybase Control Center toolbar, click the **Launch Resource Explorer** icon.
2. Select the resources to add to your perspective. Use **Shift-click** or **Control-click** to select multiple resources.
3. Perform one of these actions:
 - Select **Resources > Add Resources to Perspective**.
 - Drag and drop resources from the Resource Explorer onto the Perspective Resources view. You can select and drag multiple resources.

See also

- *Removing a Resource from a Perspective* on page 1304
- *Resources* on page 1303

Authenticating a Login Account for a Managed Resource

Specify the login account and password Sybase Control Center will use when it connects to your server or agent to collect monitoring data or manage the resource.

Perform this task for each resource registered with Sybase Control Center.

Note: You can also authenticate a server during administrative tasks like creating an alert or a collection job.

1. Connect a browser to Sybase Control Center and log in.
2. If the Perspective Resources view is not open, click the **Show/Hide Perspective Resources View** icon in the toolbar.
3. In the Perspective Resources view, select your resource and select **Resource > Authenticate** from the view menu.
4. Select **Use my current SCC login** or **Specify different credentials**.
5. If you chose **Specify different credentials**, enter the login and password for Sybase Control Center to use to connect to your resource.
6. If the selected resource is a Replication Server, also enter the RSSD user name and password.
7. Click **OK** to save and exit the dialog.

See also

- *Changing Update Frequency for Statistics and Charts* on page 282
- *User Authorization* on page 119

Match Case in sysuser for Authentication User ID

When you authenticate Sybase Control Center with an SAP Sybase IQ server, enter the user ID in the same case in which it appears in the SAP Sybase IQ server's sysuser table.

When the cases do not match, SCC authenticates the server—for example, if the sysuser entry says DBA you can authenticate as dba. You can monitor the SAP Sybase IQ server, but you cannot make changes or perform management tasks in the Administration Console.

Changing Update Frequency for Statistics and Charts

You can control the rate at which data on monitor screens and charts is refreshed, the amount of time covered by charts, and the multiplex nodes included in charts.

1. In the Perspective Resources view, select a resource, click the arrow, and select one of:

- Simplex resource – **Monitor Node**.
 - Multiplex resource – **Monitor Multiplex**.
 - Logical server resource – **Monitor Logical Server**.
2. In the left pane, select **Settings**.
 3. For **Screen Refresh Interval**, the number of seconds between refreshes. You can also use the up and down arrows to select the appropriate number of seconds.
The default is 30 seconds.
 4. For **Chart Trend Period**, the number of minutes of data to appear in charts.
The minimum number of minutes is 5, and the maximum number is 999999999. The default is 30 minutes.
Since data is added to a chart only when it is open, a chart contains data starting from when you opened it. Each refresh interval adds new data to the end of the graph. A chart trend period of 30 minutes shows the statistics trend over the last 30 minutes, even if the view has been open longer than 30 minutes.
 5. For multiplex and logical server monitoring:
 - a) For **Maximum Number of Nodes to Show in Chart**, the maximum number of nodes to include in any monitoring charts.
The default is 10 nodes.
 - b) Click **Select Nodes**, then choose the nodes to include in the monitoring charts. You cannot select more than the maximum number of nodes.
 - c) Click **OK**.
 6. Click **Apply**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Modifying the Data Collection Interval for a Job* on page 1293

Setting Up Statistics Collection

Use the Properties view of your managed resource to create a data collection job and add a schedule to the job.

Statistics gathering consumes system resources intensively; the more collection jobs you run, the greater the burden on your server. For best performance, Sybase recommends these guidelines for scheduling data collection jobs:

- Schedule only one collection job for each collection.
- Set the collection interval to 5 minutes or more. (The default is 5 minutes.)

Data collections for a managed resource do not run until the resource is authenticated.

Configure Sybase Control Center

1. In the Perspective Resources view, select a resource, click its drop-down arrow, and select **Resource > Properties**.
2. Select **Collection Jobs**.
3. Click **Create Job**.
4. If this resource has not yet been authenticated, you see the Authentication page. Enter a user name and password that Sybase Control Center can use to log in to the resource. Click **Authenticate** to verify your credentials. Data collections can run only on an authenticated resource.
5. On the Collection Information page, select the data collection that this job will run.
6. (Optional) If you do not want SCC to save data collected for this job in the repository, unselect **Save data collected from this job**.

If you choose not to save collection data, SCC updates any open views (the heat chart or a resource monitor, for example) when the job runs. If the job runs when no views are open, the data is not captured.

This option cannot be modified once the job is created. If you need to change it, drop the data collections and add it again.

7. Click **Next**.
8. (Optional) If you do not want to create a schedule yet, unselect **Create a schedule for this job**.
9. Specify details for the new schedule:

Field	Description
Name	A name for this schedule
Description	A description of this schedule

10. Choose to start the job **Now** or **Later**. If you choose **Later**, specify the start date and time.
11. Specify the duration of this schedule. The job can run:

- **Once**
- **Repetitively** at an interval you specify

Field	Description
Repeat interval	Time period (in seconds, minutes, hours, or days) between job executions

- **Until** a stop date that you specify, at an interval you specify

Field	Description
Repeat interval	Time period (in seconds, minutes, hours, or days) between job executions
Stop date	Date and time the job should stop running

Note: Enter dates and times using your local time. Sybase Control Center converts your times for remote time zones if necessary.

You cannot change the duration of a schedule (the once/repetitively/until setting) after you create it. To change the schedule duration, delete and recreate the schedule.

12. Click Finish.

See also

- *Creating an Alert* on page 295
- *Graphing Performance Counters: the Statistics Chart* on page 320
- *Job Scheduling* on page 1289
- *Viewing or Deleting a Schedule* on page 1292

About Statistics

Understand availability and performance statistics in Sybase Control Center.

The statistics you work with in Sybase Control Center can be divided into two types:

- Availability statistics are concerned with present conditions; they help you determine whether a resource you are monitoring (a server or an agent, for example) is running and functioning properly.
- Performance statistics are concerned with behavior of the same resources over time. They describe the flow of data through your environment. You can use performance statistics to spot trends, identify problems like resource bottlenecks, and make plans.

Sybase Control Center includes predefined key performance indicators (KPIs) for each product module; these KPIs are grouped into collections. KPIs such as server status, which serves as an availability statistic when it is fresh, have long-term value as historical performance statistics.

Availability statistics appear on the heat chart and on resource monitoring screens in each product module.

Performance statistics appear on the statistics chart and on resource monitoring screens in each product module.

Some KPIs are included in the default collection for each product module. To make other KPIs available to the heat chart, statistics chart, and resource monitoring views, you must set up collection jobs in the scheduler. See the data collections help topic for information on data collections and the KPIs contained in them.

Several configuration options affect the collection and display of data in Sybase Control Center:

- Collection repeat interval—The frequency of data collection. Set this on the collection job in the scheduler.

Configure Sybase Control Center

- Screen refresh interval—The period between screen refreshes. Refreshing the screen redraws it with the newest available data. Set the screen refresh interval in the product module. (May not be settable in all product modules.)
- Chart trend period—The period over which data is displayed in historical charts. Set the trend period in the product module. (May not be settable in all product modules.)

See also

- *SAP Sybase IQ Data Collections* on page 286

SAP Sybase IQ Data Collections

Predefined data collections that generate statistics for the historical data displayed in the Statistics Chart. Collected statistics appear on Sybase Control Center monitoring screens and trigger user-configured alerts.

SAP Sybase IQ provides alternative versions of several data collections to avoid duplication. The alternatives (which are all described in the tables below) are:

- All Statistics Collection and All Stats w/o Availability
- Engine Statistics Collection and Engine Stats w/o Availability
- Connection Statistics Collection and Connection Stats w/o Availability
- Cache Statistics Collection and Cache Stats w/o Availability
- All Multiplex Statistics Collection and All MPX Stats w/o Availability
- All Logical Server Statistics Collection and All Logical Server Stats w/o Availability

The “w/o Availability” collections omit statistics that are collected by the Availability Statistics Collection, the Multiplex Availability Collection, or the Logical Server Availability Collection, which are scheduled by default. They are otherwise identical to their counterparts.

Minimizing duplication:

- Reduces the occurrence of duplicate alerts
- Improves the performance of both Sybase Control Center and managed servers

A statistic is considered a duplicate only when its key performance indicator is collected more than once in the same time interval.

Table 16. Data Collections for Server-Type (Simplex) Resources

Collection	Description	KPIs
All Statistics Collection	Contains all statistics, including server availability and performance statistics.	All KPIs listed in this table.

Collection	Description	KPIs
Availability Statistics Collection	<p>Contains server availability statistics used in the heat chart.</p> <p>This is the default collection; it is automatically scheduled when you authenticate an SAP Sybase IQ simplex server.</p> <hr/> <p>Important: Leave this collection running for each monitored simplex server. Suspend it only if you schedule another collection that includes all of this collection's KPIs, such as All Statistics Collection.</p> <hr/>	<ul style="list-style-type: none"> • Server Status (Resource State) • SCC Agent Status • Total CPU Usage • System CPU Usage • User CPU Usage • IQ Memory Allocated • Catalog Cache in Use • Main Cache in Use • Temporary Cache in Use • Available Connections
All Stats w/o Availability	<p>Contains all statistics except those collected by the Availability Statistics Collection.</p> <p>Schedule this collection to collect all statistics without duplication when you also use the Availability Statistics Collection, which is scheduled by default.</p>	<p>All KPIs listed in this table with the exception of those included in the Availability Statistics Collection, above.</p>
Engine Statistics Collection	<p>Contains performance statistics for the SAP Sybase IQ engine.</p>	<ul style="list-style-type: none"> • Total CPU Usage • System CPU Usage • User CPU Usage • IQ Memory Allocated • IQ Maximum Memory Allocated • IQ Threads in Use • IQ Threads Available

Collection	Description	KPIs
Engine Stats w/o Availability	Contains all statistics in the Engine Statistics Collection except those collected by the Availability Statistics Collection. To avoid duplication with the Availability Statistics Collection, schedule this collection rather than the Engine Statistics Collection.	<ul style="list-style-type: none"> • IQ Maximum Memory Allocated • IQ Threads in Use • IQ Threads Available
Connection Statistics Collection	Contains connection performance statistics.	<ul style="list-style-type: none"> • Active Connections • Active INC Incoming Connections • Active INC Outgoing Connections • Active User Connections • Available Connections • Resumed INC Connections • Rolled back INC Connections • Suspended INC Connections • User Connections Per Minute • User Disconnections Per Minute
Connection Stats w/o Availability	Contains all statistics in the Connection Statistics Collection except those collected by the Availability Statistics Collection. To avoid duplication with the Availability Statistics Collection, schedule this collection rather than the Connection Statistics Collection.	<ul style="list-style-type: none"> • Active Connections • Active User Connections • Active INC Incoming Connections • Active INC Outgoing Connections • User Connections Per Minute • User Disconnections Per Minute
Transaction Statistics Collection	Contains transaction performance statistics.	<ul style="list-style-type: none"> • Active Transactions • Active User Transactions • Active INC Transactions • Active Load Table Statements
DBSpace Statistics Collection	Contains statistics for each dbspace.	<ul style="list-style-type: none"> • Percentage of Available DBSpace • DBSpace Size in Use

Collection	Description	KPIs
DBSpace File Statistics Collection	Contains statistics for each dbspace file.	<ul style="list-style-type: none"> Percentage of Available DBSpace File DBSpace File Size in Use
Store I/O Statistics Collection	Contains performance statistics for store reads and writes.	<ul style="list-style-type: none"> Catalog Store Disk Reads Per Second Catalog Store Disk Writes Per Second Temporary Store Disk Reads Per Second Temporary Store Disk Writes Per Second Main Store Disk Reads Per Second Main Store Disk Writes Per Second
Cache Statistics Collection	Contains performance statistics for caches.	<ul style="list-style-type: none"> Catalog Cache Hits Per Second Catalog Cache Reads Per Second Catalog Cache Size Catalog Cache in Use Catalog Cache Pinned Catalog Cache Pinned Percent Catalog Cache Dirty Pages Percent Main Cache Hits Per Second Main Cache Reads Per Second Main Cache Size Main Cache in Use Main Cache Pinned Main Cache Pinned Percent Main Cache Dirty Pages Percent Temporary Cache Hits Per Second Temporary Cache Reads Per Second Temporary Cache Size Temporary Cache in Use Temporary Cache Pinned Temporary Cache Pinned Percent Temporary Cache Dirty Pages Percent

Collection	Description	KPIs
Cache Stats w/o Availability	Contains all statistics in the Cache Statistics Collection except those collected by the Availability Statistics Collection. To avoid duplication with the Availability Statistics Collection, schedule this collection rather than the Cache Statistics Collection.	<ul style="list-style-type: none"> • Catalog Cache Hits Per Second • Catalog Cache Reads Per Second • Catalog Cache Size • Catalog Cache Pinned • Catalog Cache Pinned Percent • Catalog Cache Dirty Pages Percent • Main Cache Hits Per Second • Main Cache Reads Per Second • Main Cache Size • Main Cache Pinned • Main Cache Pinned Percent • Main Cache Dirty Pages Percent • Temporary Cache Hits Per Second • Temporary Cache Reads Per Second • Temporary Cache Size • Temporary Cache Pinned • Temporary Cache Pinned Percent • Temporary Cache Dirty Pages Percent
Op/Req Statistics Collection	Contains performance statistics related to operations and requests.	<ul style="list-style-type: none"> • IQ Waiting Operations • IQ Active Operations • Requests Per Second • Unscheduled Requests
Network Statistics Collection	Contains network-related performance statistics.	<ul style="list-style-type: none"> • Bytes Received Per Second • Bytes Received Uncompressed Per Second • Bytes Sent Per Second • Bytes Sent Uncompressed Per Second • Available Communication Buffers • Total Communication Buffers

Table 17. Data Collections for Multiplex-Type Resources

Collection	Description	KPIs
All Multiplex Statistics Collection	Contains all multiplex-related statistics and all statistics for each node. When scheduled, all node statistics are collected.	All KPIs listed in this table and, for each node, the statistics listed in the Data Collections for Server-Type (Simplex) Resources, above.
Multiplex Availability Collection	<p>Contains multiplex status, availability statistics, and multiplex role/status/failover/INC status of each node. When scheduled, all node availability statistics are collected.</p> <p>This is the default collection; it is automatically created when you authenticate a multiplex-type resource.</p> <hr/> <p>Important: Leave this collection running for each monitored multiplex server. Suspend it only if you schedule another collection that includes all of this collection's KPIs, such as All Multiplex Statistics Collection.</p> <hr/>	<ul style="list-style-type: none"> • Multiplex status • Average Available Connections (Count) • Average Catalog Cache in Use (Percent) • Average CPU Usage (Percent) • Average Main Cache in Use (Percent) • Average Temporary Cache in Use (Percent) • Maximum Available Connections (Count) • Maximum Catalog Cache in Use (Percent) • Maximum CPU Usage (Percent) • Maximum Main Cache in Use (Percent) • Maximum Temporary Cache in Use (Percent) • Minimum Available Connections (Count) • Minimum Catalog Cache in Use (Percent) • Resource State (State) • Total Available Connections (Count)

Collection	Description	KPIs
All MPX Stats w/o Availability	Contains all statistics except those collected by the Multiplex Availability Collection. Schedule this collection to collect all statistics without duplication when you also use the Multiplex Availability Collection, which is scheduled by default.	All KPIs listed in this table with the exception of those included in the Multiplex Availability Collection, above.

Table 18. Data Collections for Logical Server Resources

Collection	Description	KPIs
Logical Server Statistics Collection	Contains all logical server-related statistics and all statistics for each node. When scheduled, all logical server statistics are collected.	<p>The following KPIs for the logical server:</p> <ul style="list-style-type: none"> • Logical Server Status <p>The following KPIs for Connections:</p> <ul style="list-style-type: none"> • Average CPU Usage • Minimum CPU Usage • Maximum CPU Usage • Average Available Connections • Minimum Available Connections • Maximum Available Connections • Total Available Connections • Average User Connections • Minimum User Connections • Maximum User Connections • Total User Connections <p>The following KPIs for Transactions:</p> <ul style="list-style-type: none"> • Average User Transactions • Minimum User Transactions • Maximum User Transactions • Total User Transactions • Average Active Load Table Statements • Minimum Active Load Table Statements • Maximum Active Load Table Statements • Total Active Load Table Statements <p>The following KPIs for Caches:</p> <ul style="list-style-type: none"> • Average Catalog Cache in Use • Minimum Catalog Cache in Use • Maximum Catalog Cache in Use • Average Temporary Cache in Use • Minimum Temporary Cache in Use • Maximum Temporary Cache in Use

Collection	Description	KPIs
		<ul style="list-style-type: none"> • Average Main Cache in Use • Minimum Main Cache in Use • Maximum Main Cache in Use <p>The following KPIs for Operations and Requests:</p> <ul style="list-style-type: none"> • Average Waiting Operations • Minimum Waiting Operations • Maximum Waiting Operations • Total Waiting Operations • Average Active Operations • Minimum Active Operations • Maximum Active Operations • Total Active Operations
Logical Server Availability Statistics Collection	<p>Contains logical server status and availability statistics status of each node. When scheduled, all node availability statistics are collected.</p> <p>This is the default collection; it is automatically created when you authenticate a logical server-type resource.</p> <hr/> <p>Important: Leave this collection running for each monitored logical server. Suspend it only if you schedule another collection that includes all of this collection's KPIs, such as All Logical Server Statistics Collection.</p> <hr/>	<p>The following KPIs for the logical server:</p> <ul style="list-style-type: none"> • Logical Server Status • Average CPU Usage • Minimum CPU Usage • Maximum CPU Usage • Average Available Connections • Minimum Available Connections • Maximum Available Connections • Total Available Connections • Average Catalog Cache in Use • Minimum Catalog Cache in Use • Maximum Catalog Cache in Use • Average Temporary Cache in Use • Minimum Temporary Cache in Use • Maximum Temporary Cache in Use • Average Main Cache in Use • Minimum Main Cache in Use • Maximum Main Cache in Use

Collection	Description	KPIs
All Logical Server Stats w/o Availability	Contains all statistics except those collected by the Logical Server Availability Collection. Schedule this collection to collect all statistics without duplication when you also use the Logical Server Availability Collection, which is scheduled by default.	All KPIs listed in this table with the exception of those included in the Logical Server Availability Collection, above.

See also

- *About Statistics* on page 285
- *Creating an Alert* on page 295

Creating an Alert

Use the Add Alert wizard to create an alert instance for your resource.

Prerequisites

- You must have administrative privileges (sccAdminRole) to perform this task.
- Specify an e-mail server for Sybase Control Center to use for alerts. You cannot create e-mail subscriptions to alerts without an e-mail server.
- Schedule data collections. Alerts for each product module are based on one or more data collections. If the correct collection or collections are not scheduled to run, the alert system cannot function and no alerts are generated. See the data collections topic for your product module for information on which collections you need to schedule to enable alerts.
- (Optional) If you want this alert to trigger the execution of a shell script, copy the script to a location on or accessible from the machine that hosts your Sybase Control Center server. Set permissions to make the script executable.

Warning! Use caution in writing scripts. A poorly designed script can cause a blocking situation, creating a deadlock in your Sybase Control Center server.

Task

1. In the Perspective Resources view, click the server or other resource and select **Resource > Properties** in the view's menu bar.
2. Select **Alerts** in the left pane and click **Add**.

The Add Alert wizard opens. If the selected resource supports child alerts, the wizard opens to the Resource page. If the resource does not support child alerts, the wizard opens to the Type page—in that case, skip to step 5.

3. On the Resource page of the wizard, select the object on which to set the alert. Expand the folder representing the server or agent to select lower-level child objects.

4. Click **Next**.

5. On the Type page, select the alert type and click **Next**.

For this step and the next one, see the topic on key performance indicators for information on what this alert monitors and how it is triggered. (Each alert is based on a KPI.)

6. Based on the type of alert you selected, do one of the following:

- For a state-based alert – select a severity level for each alert state.

Note: You can associate only one severity level with each state.

- For a threshold-based alert – review and if necessary adjust the range of values that defines each severity.

7. Click **Next**.

8. (Optional) Enter the storm suppression period. Storm suppression blocks redundant alert notifications and script executions resulting from the same condition for the specified period of time. Enter this value in seconds, minutes, or hours and click **Next**.

9. (Optional) To configure this alert to trigger the execution of a script:

- a) **Alert Severity** specifies the severity level that triggers the script. Select **Critical**, **Warning**, or both.

Critical is typically more serious than Warning.

- b) Browse to the location of the script.

Note: In UNIX, make sure the script is executable. You cannot select a script unless it has execute permission.

- c) If the script requires parameter values, click **Select Parameters** to enter them in the **Execution Parameters** box.

You can include a number of predefined substitution parameters, which are replaced by values from the alert. The parameter values are passed on the command line to the script. See the example and the substitution parameters topic (linked below) for more information.

Note: When you test a script, Sybase Control Center supplies test values for the **%Severity%** and **%Source_Application%** parameters (“Testing” and “TestScriptExecution,” respectively). Any test values you supply for these parameters are discarded. This prevents the test results from being confused with real script results after testing and in the SCC repository.

- d) (Optional) Click **Test** to perform a test execution of your script.

If your script takes parameters, the test may fail if parameter values are missing or incorrect.

e) Click **Next**.

If the selected resource has sibling resources (databases or devices of the same type, for example) that support this alert type, you see the Duplicates page. If the selected resource has no identical siblings, you see the Subscription page.

10. (Optional) On the Duplicates page, select any resources that should use this alert definition as a template for their own alerts. Click the box at the top of the list to select all the resources listed. Then click **Next**.

This step saves time when you need to configure similar alerts for several resources of the same type.

11. (Optional) On the Subscription page, specify e-mail addresses if you want this alert to issue e-mail notifications when it fires.

The e-mail addresses default to the address in your user profile, but you can override the defaults.

For both critical and warning alerts:

Table 19. Alert subscription details

Option	Description
E-mail	To send an e-mail notification when this alert fires, click the E-mail Message box and enter the e-mail address of one user or list.
Escalation E-mail	To escalate this alert (by sending another e-mail notification if this alert has not been responded to after a specified period of time), click the Escalation E-mail box and enter the e-mail address of one user or list. You cannot enter an escalation address unless you enter an address for primary notification first.
Time Period	Specify how long to wait, following the initial alert notification, before Sybase Control Center sends an e-mail notification to the escalation address. (The same notification is sent again to the original notification address.) Select a time unit (hours, minutes, or seconds) and enter a number.

12. Click **Finish**.

If you are creating duplicate or child alerts, the **Cancel** button is activated; click it to interrupt the creation of further alerts. (The primary alert, at a minimum, is always created before the operation can be cancelled.) If you do not want to keep the duplicate or child alerts (if any) created before you cancelled the operation, drop them manually.

Note: Click **Cancel** to stop the creation of duplicate alerts.

See also

- *Setting Up Statistics Collection* on page 283
- *Key Performance Indicators for SAP Sybase IQ* on page 307
- *SAP Sybase IQ Data Collections* on page 286
- *Assigning a Role to a Login or a Group* on page 119
- *Configuring the E-mail Server* on page 116
- *Alerts* on page 1294
- *Testing an Alert-Triggered Script* on page 1297

SAP Sybase IQ Alerts

Alerts you can use for SAP Sybase IQ.

The alerts are based on the same key performance indicators (KPIs) that are collected for the SAP Sybase IQ node level monitor displays, and for the Statistics Chart.

Note: To configure alerts for a multiplex, register each node for which you want to set alerts and add the node to a perspective. Then set up alerts for each node using the Resource Properties view (select a server in the Perspective Resources view and select **Resource > Properties > Alerts**). Do not create alerts in the Resource Properties view for the multiplex.

Alert/KPI	Description	Alert Type
Active INC incoming connections	Number of internode communication (INC) incoming connections.	Threshold
Active INC outgoing connections	Number of INC outgoing connections.	Threshold
Active INC transactions	Number of active INC transactions.	Threshold
Active load table statements	Number of active load table statements.	Threshold
Active transactions	Total number of active transactions, including user and INC transactions.	Threshold
Active user connections	Number of active user connections.	Threshold
Active user transactions	Number of active user transactions.	Threshold
Available communication buffers	Number of available network communication buffers.	Threshold
Bytes received	Number of bytes per second received during client/server communications.	Threshold

Alert/KPI	Description	Alert Type
Bytes received uncompressed	Number of bytes per second that would have been received during client/server communications if compression was disabled.	Threshold
Bytes sent	Number of bytes per second sent during client/server communications.	Threshold
Bytes sent uncompressed	Number of bytes per second that would have been sent during client/server communications if compression was disabled.	Threshold
Catalog cache dirty pages percent	Percentage of pages in the catalog cache where data has been modified and stored in the buffer cache and has not yet been written to disk.	Threshold
Catalog cache hits	Number of catalog cache hits per second.	Threshold
Catalog cache in use percent	Percentage of the catalog cache in use.	Threshold
Catalog cache pinned	Number of pinned catalog cache pages.	Threshold
Catalog cache pinned percent	Percentage of the catalog cache pinned.	Threshold
Catalog cache reads	Number of catalog cache page lookups per second.	Threshold
Catalog store disk reads	Number of kilobytes per second that have been read from the catalog store.	Threshold
Catalog store disk writes	Number of kilobytes per second that have been written to the catalog store.	Threshold
CPU total usage	Percentage of the Sybase IQ server CPU in use, including both system and user usage.	Threshold
Dbspace size in use	<p>Dbspace size in use in MB.</p> <hr/> <p>Note: Do not configure dbspace alerts on secondary nodes in a multiplex—they do not work. Only the coordinator node can gather statistics for dbspaces and fire dbspace alerts.</p> <hr/>	Threshold

Alert/KPI	Description	Alert Type
Dbspace file size in use	<p>Dbspace file size in use in MB.</p> <hr/> <p>Note: Do not configure dbspace alerts on secondary nodes in a multiplex—they do not work. Only the coordinator node can gather statistics for dbspaces and fire dbspace alerts.</p> <hr/>	Threshold
Dbspace percent available	<p>Percentage of Dbspace size available.</p> <hr/> <p>Note: Do not configure dbspace alerts on secondary nodes in a multiplex—they do not work. Only the coordinator node can gather statistics for dbspaces and fire dbspace alerts.</p> <hr/>	Threshold
Dbspace file percent available	<p>Percentage of Dbspace file size available.</p> <hr/> <p>Note: Do not configure dbspace alerts on secondary nodes in a multiplex—they do not work. Only the coordinator node can gather statistics for dbspaces and fire dbspace alerts.</p> <hr/>	Threshold
IQ active operations	Number of active concurrent operations admitted by the SAP Sybase IQ resource governor.	Threshold
SCC Agent Availability	Indicates Sybase Control Center agent availability state. Possible values: UNKNOWN(0), STOPPED(1), and RUNNING(3).	State
IQ threads in use	Number of threads used by the SAP Sybase IQ server.	Threshold
Main cache hits	Number of main cache hits per second.	Threshold
Main cache in use percent	Percentage of the main cache in use.	Threshold
Main cache pinned	Number of pinned main cache pages.	Threshold
Main cache pinned percent	Percentage of the main cache pinned.	Threshold
Main cache reads	Number of main cache page lookups per second.	Threshold
Main cache size	Current main cache size in megabytes.	Threshold
Main store disk reads	Number of kilobytes per second that have been read from the main store.	Threshold

Alert/KPI	Description	Alert Type
Main store disk writes	Number of kilobytes per second that have been written to the main store.	Threshold
Number of active connections	Total number of active connections, including user and internode communication connections.	Threshold
Number of connections available	Number of concurrent connections available.	Threshold
Number of IQ threads available	Number of threads available in the Sybase IQ server.	Threshold
Requests per second	Number of times per second the server has been accessed to handle a new request or continue processing an existing request.	Threshold
Server availability	Status of the Sybase IQ server.	State
Temp cache dirty pages percent	Percentage of pages in the temporary caches where data has been modified and stored in the buffer cache and has not yet been written to disk.	Threshold
Temp cache hits	Number of temporary cache hits per second.	Threshold
Temp cache in use percent	Percentage of the temporary cache in use.	Threshold
Temp cache pinned	Number of pinned temporary cache pages.	Threshold
Temp cache pinned percent	Percentage of the temporary cache pinned.	Threshold
Temp cache reads	Number of temporary cache page lookups per second.	Threshold
Temp cache size	Current temporary cache size in megabytes.	Threshold
Temp store disk reads	Number of kilobytes per second that have been read from the temporary store.	Threshold
Temp store disk writes	Number of kilobytes per second that have been written to the temporary store.	Threshold
Total communication buffers	Total number of network communication buffers.	Threshold
Unscheduled requests	Number of requests that are currently queued up waiting for an available server thread.	Threshold

Alert/KPI	Description	Alert Type
User connections per minute	Number of user connections per minute.	Threshold
User disconnections per minute	Number of user disconnections per minute.	Threshold

See also

- *Alert Types and Severities for SAP Sybase IQ* on page 302
- *Alert-Triggered Scripts* on page 303
- *Alert-Triggered Script Examples* on page 304
- *Substitution Parameters for Scripts* on page 305

Alert Types and Severities for SAP Sybase IQ

Learn about the properties that define and control alerts.

An alert's type determines what causes it to fire.

Table 20. Alert types

Type	Description
State	A state alert fires when the metric on which it is based changes to a particular state. The possible states are running, pending, stopped, warning, error, and unknown.
Threshold	A threshold alert fires when the metric on which it is based passes a preset level.

Alert severities control when an alert is issued. You can configure the states or threshold values for each alert.

Table 21. Alert severities

Severity	Description
Normal	No alert is issued.
Warning	A problem has given cause for concern. An alert is issued; you can subscribe to alerts that fire at the Warning level.
Critical	A serious problem exists. An alert is issued; you can subscribe to alerts that fire at the Critical level.

See also

- *SAP Sybase IQ Alerts* on page 298

- *Alert-Triggered Scripts* on page 303
- *Alert-Triggered Script Examples* on page 304
- *Substitution Parameters for Scripts* on page 305

Alert-Triggered Scripts

You can write a shell script and configure an alert to execute the script.

Use scripts to help manage and respond to alerts. A script might trigger a visual alarm in a control center or send an e-mail message about the alert to a list of addresses (a way of supplementing the alert subscription feature, which accepts a single address).

When you configure an alert to execute a script, you:

- Specify the states or thresholds that set off the alert
- Specify the severity level that triggers execution of the script
- Supply an execution parameter string to be passed to the script

Scripts are executed under the login account used to start Sybase Control Center. Make sure that account has permissions that allow it to perform the actions contained in all scripts.

When a script executes, Sybase Control Center logs the start time, end time, and status and exit codes to the alert services log. Log location:

- In a standard installation:
`SCC-3_2\log\alert-server.log`
- In a shared disk installation:
`SCC-3_2\instances\<instance-name>\log\alert-server.log`

Warning! Use caution in writing scripts. A poorly designed script can cause a blocking situation, creating a deadlock in your Sybase Control Center server.

See also

- *SAP Sybase IQ Alerts* on page 298
- *Alert Types and Severities for SAP Sybase IQ* on page 302
- *Alert-Triggered Script Examples* on page 304
- *Substitution Parameters for Scripts* on page 305
- *Testing an Alert-Triggered Script* on page 1297
- *Alerts* on page 1294

Alert-Triggered Script Examples

Sample scripts for Windows and UNIX.

Example 1: An Alert-Triggered Windows Script

This sample script is a Windows .bat file. It outputs the parameter values you pass to it to a text file. Windows batch files support only nine arguments. (Arg0, the name of the script, is not counted.)

```
@echo off
@echo. >> stest.txt
@echo %date% %time% >> stest.txt
@echo arg0: %0 >> stest.txt
@echo arg1: %1 >> stest.txt
@echo arg2: %2 >> stest.txt
@echo arg3: %3 >> stest.txt
@echo arg4: %4 >> stest.txt
@echo arg5: %5 >> stest.txt
@echo arg6: %6 >> stest.txt
@echo arg7: %7 >> stest.txt
@echo arg8: %8 >> stest.txt
@echo arg9: %9 >> stest.txt
@echo. >> stest.txt
```

This is a sample execution parameter string for the script above:

```
Time:%Time%
Severity:%Severity%
Resource:%Resource%
Server:%Top_resource%
KPI:%KPI%
State:%Current_state%
URL:%SCC_URL%
```

The script's output might look like this:

```
Tue 12/15/2009 14:54:45.58
arg0: C:\project\sccmain\script-test.bat
arg1: Time:"Mon Dec 21 21:30:04 2009"
arg2: Severity:CRITICAL
arg3: Resource:"SCC Tester 1"
arg4: Server:"SCC Tester 1"
arg5: KPI:kpi_scc_mostate_primary
arg6: State:ERROR_
arg7: HYPERLINK "http://ik-scc.sybase.com:8282/scc"URL:http://ik-
scc.sybase.com:8282/scc
arg8:
arg9:
```

Example 2: An Alert-Triggered UNIX Script

This is a UNIX script. Like the Windows script above, it outputs the parameter values you pass to it to a text file.


```
#!/bin/sh
outfile=/testing/latest/scriptTest.out
echo> $outfile
echo `date` >> $outfile
count=1
while [ "$1" ]
do
    echo arg$count: $1 >> $outfile
    shift
    count=`expr $count + 1`
done
echo --- DONE --- >> $outfile
```

See also

- *SAP Sybase IQ Alerts* on page 298
- *Alert Types and Severities for SAP Sybase IQ* on page 302
- *Alert-Triggered Scripts* on page 303
- *Substitution Parameters for Scripts* on page 305

Substitution Parameters for Scripts

In the execution parameter string you supply to be passed to your shell script, you can include substitution parameters that are replaced at execution time with values from the alert that triggers the script.

Substitution parameters are available for both state-based and threshold-based alerts.

Table 22. Substitution Parameters for State-Based Alerts

Parameter	Description
%Alert%	A three-part name supplied by the alert system. The parts are the name of this alert, the name of the resource, and the name of the key performance indicator (KPI) on which this alert is based.
%Current_state%	The current state of the resource on which this alert is configured.
%KPI%	The name of the KPI on which this alert is based.
%Resource%	The name of the resource with which this alert is associated.
%SCC_URL%	A link to Sybase Control Center, where more information about the alert may be available.
%Severity%	The severity of this alert: critical or warning.
%Source_application%	The SCC product module that generated this alert.

Parameter	Description
%Time%	The date and time at which the alert fired, in this format: Tue Sep 15 10:10:51 2009
%Server%	The name of the alerted resource's top-level parent resource—usually the server. This is valuable when the alerted resource is a component of a larger system (a database in a server, for example). If the alerted resource has no parent, %Server% and %Resource% have the same value.

Table 23. Substitution Parameters for Threshold-Based Alerts

Parameter	Description
%Alert%	A three-part name supplied by the alert system. The parts are the name of this alert, the name of the resource, and the name of the key performance indicator (KPI) on which this alert is based.
%Datapoint%	The current value, on the alerted resource, of the KPI on which this alert is based.
%KPI%	The name of the KPI on which this alert is based.
%Resource%	The name of the resource with which this alert is associated.
%SCC_URL%	A link to Sybase Control Center, where more information about the alert may be available.
%Severity%	The severity of this alert: critical or warning. (Critical is more serious.)
%Source_application%	The SCC product module that generated this alert.
%Threshold%	The threshold value at which this alert fires.
%Time%	The date and time at which the alert fired, in this format: Tue Sep 15 10:10:51 2009
%Server%	The name of the alerted resource's top-level parent resource. This is valuable when the alerted resource is a component of a larger system (a database in a server, for example). If the alerted resource has no parent, %Server% and %Resource% have the same value.

See also

- *SAP Sybase IQ Alerts* on page 298
- *Alert Types and Severities for SAP Sybase IQ* on page 302

- *Alert-Triggered Scripts* on page 303
- *Alert-Triggered Script Examples* on page 304
- *Testing an Alert-Triggered Script* on page 1297
- *Modifying an Alert* on page 1297

Key Performance Indicators for SAP Sybase IQ

Key performance indicators (KPIs) provide the statistics that appear on SAP Sybase IQ screens and charts in Sybase Control Center.

Each SAP Sybase IQ data collection includes a subset of the KPIs listed here.

Table 24. SAP Sybase IQ Availability Statistics

KPI	Description
Server Status (Resource State)	Status of the SAP Sybase IQ server. Valid states are: <ul style="list-style-type: none"> • UNKNOWN (0) • STOPPED (1) • PENDING (2) • RUNNING (3) • WARNING (4) • ERROR (5)
Total CPU Usage	SAP Sybase IQ server total CPU usage percentage, including both system and user usage.
CPU System Usage	SAP Sybase IQ server system CPU usage percentile.
CPU User Usage	SAP Sybase IQ server user CPU usage percentile.
IQ Memory Allocated	Memory allocated by the SAP Sybase IQ server, in megabytes.
Catalog Cache in Use	Percentage of catalog cache in use.
Temporary Cache in Use	Percentage of temporary cache in use.
Main Cache in Use	Percentage of main cache in use.
Available Connections	Number of concurrent connections available.

Table 25. Sybase Control Center Agent Availability Statistics

KPI	Description
SCC Agent Status (Resource State)	<p>Status of the registered and authenticated SCC agent that enables SCC to manage the SAP Sybase IQ server. Valid states are:</p> <ul style="list-style-type: none"> UNKNOWN (0) STOPPED (1) PENDING (2) RUNNING(3) WARNING (4) ERROR (5)

Table 26. Multiplex Availability Statistics

KPI	Description
Multiplex Status (Resource State)	<p>Status of the multiplex. Valid states are:</p> <ul style="list-style-type: none"> UNKNOWN (0) STOPPED (1) (A multiplex is considered stopped if there is no running node.) PENDING (2) RUNNING (3) (A multiplex is considered to be running if at least one node is running.) WARNING (4) ERROR (5)

Table 27. Multiplex Node Properties

KPI	Description
Multiplex Role (Resource Secondary State)	<p>Indicates the multiplex role of the node. Valid states are:</p> <ul style="list-style-type: none"> COORDINATOR (0) WRITER (1) READER (2) SINGLE_SERVER (3)

KPI	Description
Multiplex Status	Indicates the multiplex status of the node. Valid values are: <ul style="list-style-type: none"> INCLUDED (0) EXCLUDED (1)
Multiplex Failover Node	Indicates whether the node is a designated fail-over node. Valid values are: <ul style="list-style-type: none"> FALSE (0) TRUE (1)

Table 28. Multiplex Link Availability Statistics

KPI	Description
INC Status (Resource State)	Status of internode communication between a secondary node and the coordinator. Valid states are: <ul style="list-style-type: none"> UNKNOWN (0) STOPPED (1) PENDING (2) ACTIVE (3) WARNING (4) ERROR (5)

Table 29. Overview Statistics

KPI	Description
Server Status	Server state or status. Valid values are: <ul style="list-style-type: none"> UNKNOWN (0) STOPPED (1) PENDING (2) RUNNING (3) WARNING (4) ERROR (5)
Total CPU Usage	SAP Sybase IQ server total CPU usage percentage, including both system and user usage.

KPI	Description
IQ Memory Allocated	Memory allocated by the SAP Sybase IQ server, in megabytes.
Number of Active Connections	Total number of active connections including user and internode-communication connections.

Table 30. Engine Statistics

KPI	Description
Total CPU Usage	SAP Sybase IQ server total CPU usage percentage, including both system and user usage.
CPU System Usage	SAP Sybase IQ server system CPU usage percentile.
CPU User Usage	SAP Sybase IQ server user CPU usage percentile.
IQ Memory Allocated	Memory allocated by the SAP Sybase IQ server, in megabytes.
IQ Maximum Memory Allocated	Maximum memory allocated by the SAP Sybase IQ server, in megabytes.
IQ Threads in Use	Number of threads used by the SAP Sybase IQ server.
IQ Threads Available	Number of threads available in the SAP Sybase IQ server.

Table 31. Connection Statistics

KPI	Description
Active Connections	Total number of active connections including user and internode communication connections.
Active INC Incoming Connections	Number of internode communication incoming connections.
Active INC Outgoing Connections	Number of internode communication outgoing connections.
Active User Connections	Number of active user connections.
Available Connections	Number of concurrent connections available.

KPI	Description
Resumed INC Connections	Number of resumed internode communication connections since server startup.
Rolled back INC Connections	On the writer, the number of rolled back global DML transactions due to INC failure. On the coordinator, the number of dropped INC connections that have been suspended.
Suspended INC Connections	Number of suspended internode communication connections since server startup.
User Connections Per Minute	Number of user connections per minute.
User Disconnections Per Minute	Number of user disconnections per minute.

Table 32. Transaction Statistics

KPI	Description
Active Transactions	Total number of active transactions, including user and INC transactions.
Active User Transactions	Number of active user transactions.
Active INC Transactions	Number of active internode communication transactions.
Active Load Table Statements	Number of active LOAD TABLE statements.

Table 33. DBSpace and DBSpace File Statistics

KPI	Description
Percentage of Available DBSpace	Percentage of the dbspace that is available.
DBSpace Size in Use	Dbspace size in use (MB).
Percentage of Available DBSpace File	Percentage of space available in the dbfile.
DBSpace File Size in Use	Dbfile size in use (MB).

Table 34. Store Input and Output Statistics

KPI	Description
Catalog Store Disk Reads Per Second	Number of kilobytes per second that have been read from the catalog store.

KPI	Description
Catalog Store Disk Writes Per Second	Number of kilobytes per second that have been written to the catalog store.
Temporary Store Disk Reads Per Second	Number of kilobytes per second that have been read from the temporary store.
Temporary Store Disk Writes Per Second	Number of kilobytes per second that have been written to the temporary store.
Main Store Disk Reads Per Second	Number of kilobytes per second that have been read from the main store.
Main Store Disk Writes Per Second	Number of kilobytes per second that have been written to the main store.

Table 35. Cache Statistics

KPI	Description
Catalog Cache Hits Per Second	Number of catalog cache hits per second.
Catalog Cache Reads Per Second	Number of catalog cache page lookups per second.
Catalog Cache Size	Current catalog cache size, in megabytes.
Catalog Cache in Use	Percentage of catalog cache in use.
Catalog Cache Pinned	Number of pinned catalog cache pages.
Catalog Cache Pinned Percent	Percentage of catalog cache pinned.
Catalog Cache Dirty Pages Percent	Percentage of catalog cache dirty pages.
Temporary Cache Hits Per Second	Number of temporary cache hits per second.
Temporary Cache Reads Per Second	Number of temporary cache page lookups per second.
Temporary Cache Size	Current temporary cache size, in megabytes.
Temporary Cache in Use	Percentage of temporary cache in use.
Temporary Cache Pinned	Number of pinned temporary cache pages.
Temporary Cache Pinned Percent	Percentage of temporary cache pinned.
Temporary Cache Dirty Pages Percent	Percentage of temporary cache dirty pages.
Main Cache Hits Per Second	Number of main cache hits per second.

KPI	Description
Main Cache Reads Per Second	Number of main cache page lookups per second.
Main Cache Size	Current main cache size, in megabytes.
Main Cache in Use	Percentage of main cache in use.
Main Cache Pinned	Number of pinned main cache pages.
Main Cache Pinned Percent	Percentage of main cache pinned.
Main Cache Dirty Pages Percent	Percentage of main cache dirty pages.

Table 36. Operations and Requests Statistics

KPI	Description
IQ Waiting Operations	Number of SAP Sybase IQ operations waiting for the resource governor.
IQ Active Operations	Number of active concurrent operations admitted by the SAP Sybase IQ resource governor.
Requests Per Second	Number of times per second the server has been entered to allow it to handle a new request or continue processing an existing request.
Unscheduled Requests	Number of requests that are currently queued up waiting for an available server thread.

Table 37. Network Statistics

KPI	Description
Bytes Received Per Second	Number of bytes per second received during client/server communications.
Bytes Received Uncompressed Per Second	Number of bytes per second that would have been received during client/server communications if compression was disabled.
Bytes Sent Per Second	Number of bytes per second sent during client/server communications.
Bytes Sent Uncompressed Per Second	Number of bytes per second that would have been sent during client/server communications if compression was disabled.

KPI	Description
Available Communication Buffers	Number of available network communication buffers.
Total Communication Buffers	Total number of network communication buffers.

Table 38. Logical Server Availability Statistics

KPI	Description
Logical Server Status	<p>Status of the logical server.</p> <ul style="list-style-type: none"> • RUNNING – at least one member node is running. • STOPPED – all member nodes are stopped. • UNKNOWN – the logical server source is unauthenticated.

Table 39. Logical Server Engine Statistics

KPI	Description
Average CPU Usage	Average CPU usage for both system and users over all member nodes.
Minimum CPU Usage	Minimum CPU usage for both system and users over all member nodes.
Maximum CPU Usage	Maximum CPU usage for both system and users over all member nodes.

Table 40. Logical Server Connection Statistics

KPI	Description
Average Available Connections	Average number of concurrent connections available over all member nodes.
Minimum Available Connections	Minimum number of concurrent connections available over all member nodes.
Maximum Available Connections	Maximum number of concurrent connections available over all member nodes.
Total Available Connections	Total number of concurrent connections available over all member nodes.

KPI	Description
Average User Connections	Average number of active user connections over all member nodes.
Minimum User Connections	Minimum number of active user connections over all member nodes.
Maximum User Connections	Maximum number of active user connections over all member nodes.
Total User Connections	Total number of active user connections available over all member nodes.

Table 41. Logical Server Transaction Statistics

KPI	Description
Average User Transactions	Average number of active user transactions available over all member nodes.
Minimum User Transactions	Minimum number of active user transactions available over all member nodes.
Maximum User Transactions	Maximum number of active user transactions available over all member nodes.
Total User Transactions	Total number of active user transactions available over all member nodes.
Average Active Load Table Statements	Average number of active load table statements over all member nodes.
Minimum Active Load Table Statements	Minimum number of active load table statements over all member nodes.
Maximum Active Load Table Statements	Maximum number of active load table statements over all member nodes.
Total Active Load Table Statements	Total number of active load table available over all member nodes.

Table 42. Logical Server Cache Statistics

KPI	Description
Average Catalog Cache in Use	Average percentage of catalog cache in use over all member nodes.

KPI	Description
Minimum Catalog Cache in Use	Minimum percentage of catalog cache in use over all member nodes.
Maximum Catalog Cache in Use	Maximum percentage of catalog cache in use over all member nodes.
Average Temporary Cache in Use	Average percentage of temporary cache in use over all member nodes.
Minimum Temporary Cache in Use	Minimum percentage of temporary cache in use over all member nodes.
Maximum Temporary Cache in Use	Maximum percentage of temporary cache in use over all member nodes
Average Main Cache in Use	Average percentage of main cache in use over all member nodes.
Minimum Main Cache in Use	Minimum percentage of main cache in use over all member nodes.
Maximum Main Cache in Use	Maximum percentage of main cache in use over all member nodes

Table 43. Logical Server Operations and Requests Statistics

KPI	Description
Average Waiting Operations	Average number of SAP Sybase IQ operations waiting for the resource governor over all member nodes.
Minimum Waiting Operations	Minimum number of SAP Sybase IQ operations waiting for the resource governor over all member nodes.
Maximum Waiting Operations	Maximum number of SAP Sybase IQ operations waiting for the resource governor over all member nodes.
Total Waiting Operations	Total number of SAP Sybase IQ operations waiting for the resource governor over all member nodes.
Average Active Operations	Average number of active concurrent operations admitted by the SAP Sybase IQ resource governor over all member nodes.
Minimum Active Operations	Minimum number of active concurrent operations admitted by the SAP Sybase IQ resource governor over all member nodes.

KPI	Description
Minimum Active Operations	Maximum number of active concurrent operations admitted by the SAP Sybase IQ resource governor over all member nodes.
Total Active Operations	Total number of active concurrent operations admitted by the SAP Sybase IQ resource governor over all member nodes.

See also

- *Creating an Alert* on page 295
- *Graphing Performance Counters: the Statistics Chart* on page 320

Optional Configuration Steps

Perform additional configuration, including user authorization, alerts, data collection scheduling, backups, and setting purging options for the repository.

Table 44. Configuration areas

Configuration area	Description	Topic
User authorization	Set up groups of users or assign roles. Make sure there are users with administrative privileges (sccAdminRole).	<i>User Authorization</i> on page 119
Authentication	Add authentication modules to allow Windows, UNIX, and LDAP users to log in to Sybase Control Center.	<i>Setting up Security</i> on page 96
Alerts	Modify alert thresholds and subscriptions and delete alerts.	<i>Alerts</i> on page 1294
Data collection	Modify collection intervals and schedules, suspend and resume the schedule, and delete collection jobs.	<i>Job Scheduling</i> on page 1289
Resources	Unregister resources, add them to perspectives, or remove them.	<i>Resources</i> on page 1303
Perspectives	Create, remove, and rename perspectives.	<i>Perspectives</i> on page 1306

Configure Sybase Control Center

Configuration area	Description	Topic
Instances	Enable or disable shared-disk mode and deploy, remove, refresh, or convert SCC agent or server instances running from a shared disk.	<i>Instances</i> on page 1310
Repository	Set purging options and schedule backups of the repository database.	<i>Repository</i> on page 1320

Administer and Monitor SAP Sybase IQ

Manage and monitor all single-node and multiplex servers in the SAP Sybase IQ environment.

Displaying Resource Availability: the Heat Chart

Use the heat chart to view the status and availability of servers in the current perspective.

The heat chart displays the state of resources in your perspective—whether the resources are running, suspended, or down. In addition, the heat chart lists the type of each resource and provides statistical data, including the start time of the last data collection.

You can filter the resources that you want to see and search and sort the results by column. You can also select a resource and pull down its context menu to see monitoring and administrative options that vary based on the resource type.

Heat chart data is collected directly from managed servers, tagged with the date and time when it was collected, and stored in the Sybase Control Center repository.

1. From the application menu bar, select **View > Open > Heat Chart**.
2. (Optional) To display information about the status represented by an icon in the chart, hover the mouse over the icon.
 - Status column – icon tooltips describe the status of the resource (Running or Stopped, for example).
 - All columns to the right of Status – icon tooltips give the value of the KPI listed at the top of the column.
3. (Optional) To display tools for filtering (narrowing the list of resources in the heat chart) or changing the columns, select **View > Filter** from the Perspective Heat Chart menu bar. The Filter and Column tools appear in the left pane.
4. (Optional) To use filtering, select **View > Filter** from the view's menu bar and enter a search term in the **Filter string** field.

The search term can be any string that appears in the tabular portion of the heat chart, such as the name, or part of the name, of a server or a resource type (ASE Server, for example).
5. (Optional) Select a filtering setting:
 - **Match case** – search for resources whose displayed data includes the search term, including uppercase and lowercase letters; or
 - **Exact match** – search for resources whose displayed data includes an item identical to the search term.
6. (Optional) Select a column from the **Filter on** list to restrict your search to that column.
7. (Optional) Click **Columns** to customize your heat chart.

8. (Optional) Unselect any column that should not appear in your heat chart.
9. (Optional) Click the sorting arrow in the column headers to sort the column values in either ascending or descending order.
10. (Optional) Click the resource's row and pull down the menu to the right of the resource name to view options for the selected resource.
11. (Optional) To resize the Filter and Columns tools pane, move your mouse over the border between the tools pane and the resource table. When the mouse cursor changes to a resize icon, click and drag the border to the left or the right.
12. (Optional) To hide the Filter and Columns tools, unselect **View > Filter**.

Graphing Performance Counters: the Statistics Chart

To show performance trends, generate a graph for any set of performance counters over a specified period of time.

Prerequisites

Verify that statistical data to be graphed has been collected. To verify data collection, go to the Collection Jobs page of the Resource Properties view and check the History tab for a collection job. You can also look at the resource monitor: if data appears there, data is being collected.

Task

Tip: Data collections start running when a resource is authenticated. A recently authenticated resource might not have accumulated enough data to make a useful graph.

1. In the Perspective Resources view, click a resource and select **Resource > Statistics Chart** in the view menu bar.
2. Expand the folders in the Statistics tab and select the key performance indicator (KPI) you want to graph.
3. Click **Graph Statistic** or drag the KPI onto the Chart tab.
The Chart tab displays the graphed data, while the KPI with its corresponding value and the date and time it was collected appear in the Data tab.
4. (Optional) Repeat to add KPIs to the graph.
5. (Optional) Use the slider at the bottom of the Chart tab to control the amount of time covered by the graph, ranging from a minute to a year.
6. (Optional) Use <<, <, >, and >> to move the displayed graph to an earlier or later time. Increments depend on how the slider is set.

Tip: The statistics chart displays data covering a fixed period of time, and that period does not change automatically. If you are viewing the most recent statistics and want to keep the graph current, adjust the displayed time period as new statistics are collected.

7. (Optional) You can click the date/time labels that appear above the slider. Use these to change the start and end time and the chart time span.
8. (Optional) Click **Clear Graph** to remove all the graphed statistics and start anew.

Note: You can graph a maximum of five statistics with no more than two distinct units of measure. By default, only 24 hours of statistics are available; change the repository purge options to save statistics for a longer period.

See also

- *Setting Up Statistics Collection* on page 283
- *Key Performance Indicators for SAP Sybase IQ* on page 307
- *Configuring Repository Purging* on page 1324

Administration Console

Use the Administration Console to browse and manage the selected resources in a perspective.

Browsing and Managing Resources

Create new resources or browse and manage existing resources.

Prerequisites

If you want to view or manage existing resources, register at least one resource and add it to a perspective.

Task

The Administration Console enables you to view and manage both servers and resources below the server level, such as processes, databases, and devices.

1. Launch the Administration Console.
 - To populate the Administration Console with information on one or more resources: in the Perspective Resources view, select the resources and select **Resource > Administration Console**. This method is the most efficient because it displays only selected resources.
 - To populate the Administration Console with information on all the resources in the current perspective: from the main menu bar, select **View > Open > Administration**

Console. If you are monitoring a large number of resources, the Administration Console may take a few minutes to load.

2. To explore the hierarchy of object types, select **Navigation > Browse** in the left pane. Expand an object type by clicking its arrow icon.

3. Select an object type (any server type, for example) in the hierarchy.

In the right pane, the Administration Console displays a list of resources of that type.

Note: Message rows in the right pane are placeholders for:

- Failed requests – to retry, select the message row and click the drop-down arrow that appears to the right. Select **Retry**.
- Slow-responding requests – SCC replaces these rows with real data as soon as it arrives.
- Large result sets – to display, select the message row and click the drop-down arrow that appears to the right. Select **Expand**. The results might take a minute to appear.

Hover the mouse over a message row to see a tooltip with more information.

4. (Optional) To create an object of the type now selected, click **Folder > Create** or **Folder > New**.
5. (Optional) To refresh the view, select **Folder > Refresh**.
6. In either the right or the left pane, select an object.
A dropdown arrow appears to the right of the name. If the selected object is in the right pane, the **Resource** menu becomes active.
7. Click the dropdown arrow to display a menu of actions you can perform on that object. If the selected object is in the right pane, use the **Resource** menu to display the same actions.

Note: Some managed objects have no actions.

See also

- *Searching and Filtering Resources* on page 322
- *Features Not Supported by a Database Version* on page 324

Searching and Filtering Resources

Use the Administration Console's search and filter tools to quickly find the resources or objects within resources that interest you.

1. Launch the Administration Console.

- To populate the Administration Console with information on one or more resources: in the Perspective Resources view, select the resources and select **Resource > Administration Console**. This method is the most efficient because it displays only selected resources.
- To populate the Administration Console with information on all the resources in the current perspective: from the main menu bar, select **View > Open > Administration**

Console. If you are monitoring a large number of resources, the Administration Console may take a few minutes to load.

2. (Optional) You can use the Administration Console's tools to control which resources it displays:
 - a) In the left pane, click **Resource Selection**.
 - b) SCC refreshes the list of resources in the right pane with each selection you make in this pane. If you are making multiple selection changes, unselect **Automatically refresh details** to turn the refresh feature off.
 - c) Select or unselect resources to include or eliminate them from Administration Console displays.
3. To find a resource without navigating the hierarchy:
 - a) In the left pane, select **Navigation > Search**.
 - b) (Required) On the Search tab, select the resource type and object type of the resource you want to find.
 - c) Enter a search string.
The search string can be the full or partial name of a resource.
 - d) (Optional) Select **Exact match** to find only the resource whose name is identical to the search string.
 - e) Click **Search**.
Results appear in the right pane.

Note: Message rows in the right pane are placeholders for:

- Failed requests – to retry, select the message row and click the drop-down arrow that appears to the right. Select **Retry**.
- Slow-responding requests – SCC replaces these rows with real data as soon as it arrives.
- Large result sets – to display, select the message row and click the drop-down arrow that appears to the right. Select **Expand**. The results might take a minute to appear.

Hover the mouse over a message row to see a tooltip with more information.

- f) To further narrow your search, enter a filter string in the field at the top of any column of search results. For example, in a search for databases, enter `wilma` above the Device column to display only results associated with the device `wilma`.

See also

- *Browsing and Managing Resources* on page 321
- *Features Not Supported by a Database Version* on page 324
- *Configuring Retrieval Thresholds for the Administration Console* on page 118

Features Not Supported by a Database Version

Sybase Control Center administration supports SAP Sybase IQ database versions 15.3 or later; however, not all features are supported by all database versions.

The behavior of features and options in the Administration Console varies, depending on the database version of the selected managed resource.

Unsupported appears in the right pane for a feature not supported by the selected managed resource.

When creating a new object, the resource drop-down list in the Create wizard includes all selected managed resources, regardless of database version. If the selected resource does not support the feature, an error message appears, and the wizard cannot proceed.

Finally, some functionality within an otherwise supported feature may not be supported. When this occurs, the corresponding page in the wizard or view is unavailable with a message indicating the feature is not supported

See also

- *Browsing and Managing Resources* on page 321
- *Searching and Filtering Resources* on page 322

Executing a SQL Query

Execute an ad hoc SQL query or a stored procedure against one or more SAP Sybase IQ servers.

You can use the Execute SQL view to execute any valid SQL statement, including queries and stored procedures. Anyone can launch a query; no permissions are required. However, if you do not have authority (15.3, 15.4) or system privilege (16.0) to perform the actions in the query, you will see an error. The query executes with the user's current permissions.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane of the Administration Console, select **IQ Servers**.
3. In the right pane, select the SAP Sybase IQ resources.
4. From the Administration Console menu bar, select **Resource > Execute SQL**.
The Execute SQL view appears.
5. In the SQL Statements box, enter a query or the name of a stored procedure and click **Execute**.

The query runs on all the SAP Sybase IQ servers you selected and results appear in the bottom portion of the view. If you selected more than one server, the view includes a results tab for each simplex or multiplex node. On the tabs,

- A green check indicates a successful query.
- A red X indicates an error.

Simplex Servers

Manage and monitor single-node in the SAP Sybase IQ environment.

Monitor Simplex Servers

Statistics allow you to monitor the availability and performance of a simplex server.

Viewing Overview Statistics

Display high-level statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Overview**.
3. Select the tab for the required information.

Note: Click a column header to sort the data by that column.

To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Tab	Description
Server	<p>State – current status of the server. Valid states include:</p> <ul style="list-style-type: none"> • Unknown • Stopped • Running <p>Host – host name where the server is running.</p> <p>Port – port number where the server is running.</p> <p>Server name – name of the server.</p> <p>Database – name of the SAP Sybase IQ database.</p> <p>Server type – type of server the database is on. Server types include Single Server, Coordinator, Reader, and Writer.</p> <p>Server version – version of the SAP Sybase IQ server.</p> <p>Platform – operating system running on the server host.</p>
Activities	<p>CPU total usage (%) – total CPU usage percentage, including both system and user usage.</p> <p>Active connections – total number of active connections, including user and internode communication connections.</p> <p>Connections available – number of connections available for users and internode communication connections.</p> <p>Active requests – number of active requests on the server.</p> <p>IQ threads in use – number of threads being used by the SAP Sybase IQ server.</p> <p>Active transactions – number of active transactions.</p> <p>Number of committed transactions – number of committed transactions.</p> <p>Oldest transaction (minutes) – elapsed age, in minutes, of the oldest transaction.</p>
Caches	<p>Catalog cache reads (per second) – number of catalog cache page lookups per second.</p> <p>Main cache size (MB) – size of the main cache, in megabytes.</p> <p>Temp cache size (MB) – size of the temporary cache, in megabytes.</p> <p>Remaining heap size (MB) – size of the remaining heap allocation, in megabytes.</p>

Tab	Description
Version usage	<p>Number of committed versions – the number of table versions in the server.</p> <p>Total version space used (MB) – total space consumed by all the table versions.</p> <p>Oldest version ID – the oldest version identifier on the server.</p> <p>Number of active versions – total number of active write table versions on the server.</p> <p>Total active version space created (MB) – amount of data created by active write transactions.</p> <p>Total active version space to be destroyed (MB) – amount of data destroyed by active write transactions. If these transactions commit, the destroyed data becomes an old version and is eventually dropped. If the transactions roll back, the created data is released.</p>
Details	<p>Server full version – version of the IQ server software, including the date and time.</p> <p>Platform version – version of the operating system installed on the server host.</p>
Alerts	Any alerts for the selected server. While the monitor is open, alerts are displayed as they are created.
CPU history chart	Percentage of total CPU usage over a period of time.
IQ memory chart	Allocation of the IQ memory between the main cache, temporary cache, and remaining heap.
Disk usage chart	Available and used space for the main and temporary stores.

See also

- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343

- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346
- *Viewing Multiplex Overview Statistics* on page 366

Viewing All Statistics

Display all the statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **All statistics**.
For each group of statistics, expand the heading to list the individual key performance indicators (KPIs) in that group. The list shows:
 - Name of the KPI
 - Current value of the KPI
 - Unit of the value
 - Description of the KPI

See also

- *Viewing Overview Statistics* on page 325
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346

Viewing Engine Statistics

Display the engine statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Engine**.

Note: To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
Engine statistics table	<p>Displays the statistics for the engine. The calculations are continuously updated based on live server information. The engine statistics include:</p> <p>CPU total usage – Percentage of CPU total usage.</p> <p>CPU system usage – Percentage of CPU system usage.</p> <p>CPU user usage – Percentage of CPU user usage.</p> <p>Total memory allocated (MB) – Total amount of memory (in megabytes) allocated for the main cache, temporary cache, and remaining heap.</p> <p>Max memory allocated (MB) – Maximum amount of memory (in megabytes) allocated for the main cache, temporary cache, and remaining heap.</p> <p>Main cache (MB) – Total size of the main cache, in megabytes.</p> <p>Temp cache (MB) – Total size of the temporary cache, in megabytes.</p> <p>IQ threads in use – Number of IQ threads in use.</p> <p>IQ threads available – Number of available IQ threads.</p>
IQ memory chart	Shows the allocation of the IQ memory between the main cache, temporary cache, and remaining heap.
CPU history chart	Displays the percentage of total, system, and user CPU usage over a period of time.

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344

- *Viewing Monitor Settings Details* on page 346

Viewing Connection Statistics

Display the connection statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Connections**.
3. Select the tab for the required information.

Note: To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
Connections tab > Active connections	<p>Displays all users currently connected to the server, including:</p> <p>User ID – the ID of the connected user.</p> <p>Name – the name of the connected user.</p> <p>Creation time – the date and time the connection was established.</p> <p>Connection ID – the ID of the connection.</p> <p>State – the current state of the selected connection. Possible states include:</p> <ul style="list-style-type: none">• ACTIVE – the connection is live.• SUSPENDED – the connection and its corresponding transaction are suspended, probably due to hardware or communication failure. <p>Client IP address – the IP address of the client that made the connection.</p> <p>Connection or cursor – indicates a connection or an active cursor</p>

Area	Description
Connections tab > Connection details	<p>Select a User ID to display that user's specific connection details, including:</p> <p>Statement being executed – the statement executed by the selected user.</p> <p>Last request time – the last time a request was executed on the server by the selected user.</p> <p>Request type – type of request executed by the selected user.</p> <p>Last command time – the last time a command was executed on the server by the selected user.</p> <p>Command type – type of command executed by the selected user.</p> <p>IQ temporary store usage (KB) – number of temporary store kilobytes used during the connection.</p> <p>IQ temporary work space usage (KB) – number of temporary workspace kilobytes used during the connection.</p> <p>Cursor count – number of open SAP Sybase IQ cursors on the connection.</p> <p>Thread in use – number of threads in use by the selected user.</p>
Connections tab > Associated transactions	Displays the transaction ID, creation time, and state of transactions executed by the selected user.
Connection Statistics tab > Active connections	Displays a chart of the number of user, internode incoming, and other connections to the server.
Connection Statistics tab > User connections/disconnections per minute	Displays the number of user connections and disconnections per minute.

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339

- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346
- *Viewing Multiplex Connection Statistics* on page 374

Viewing Transaction Statistics

Display transaction statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Transactions**.
3. Select the tab for the required information.

Note: Click a column header to sort the data by that column.

To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
Transactions tab > Transactions & versions	Displays all transactions that are currently on the server, and their version details.

Area	Description
Transactions tab > Transaction details	<p>Transaction details include:</p> <p>Transaction ID – the unique identification number for the selected transaction.</p> <p>Connection ID – the connection identification number for the selected transaction.</p> <p>Statement being executed – the statement executed by the selected transaction.</p> <p>IQ main store space created by transaction (KB) – the amount of main store space created by the selected transaction.</p> <p>IQ main store space dropped by transaction (KB) – the amount of main store space dropped by the selected transaction.</p> <p>IQ temporary store space created by transaction (KB) – the amount of temporary store space created by the selected transaction.</p> <p>IQ temporary store space dropped by transaction (KB) – the amount of temporary store space created by the selected transaction.</p> <p>Cursor count – number of open SAP Sybase IQ cursors on the transaction.</p> <p>IQ threads – number of threads being used by the transaction.</p> <p>IQ govern priority – numeric priority of the transaction in the queue.</p> <p>Connection or cursor – identifies whether the transaction is a connection or a cursor.</p> <p>Connection or cursor create time – date and time the connection or cursor was created.</p>
Transaction statistics tab > Active transactions	Displays a chart of the number of user, internode communication (identified on the chart as INC), and other transactions on the server.

Area	Description
Transaction statistics tab > Other statistics	<p>Displays additional details on the transaction, including:</p> <p>Number of committed transactions – total number of committed transactions on the server.</p> <p>Number of active load statements – total number of active load statements on the server.</p> <p>Oldest active transaction time (minutes) – elapsed time, in minutes, since the oldest active transaction's creation.</p>

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346
- *Viewing Multiplex Transaction Statistics* on page 375

Viewing Dbspaces Statistics

View dbspace size and usage details for a single server, or for a node in a multiplex, including shared temporary dbspaces.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Dbspaces**.
3. In the Dbspaces view, highlight the dbspace name to show its information in the Dbspace Details pane.

The Dbspace Details pane displays Dbspace size, and Percent available. The Size Details tab show a pie chart comparing Dbspace size in use to size available. The DB Files pane shows all the DB files that are part of highlighted Dbspace.

4. If multiple DB files appear in the DB Files pane, highlight the DB file to show its information in the DB File Details pane.

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346

Viewing Store I/O Statistics

Display the store I/O statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Store I/O**.

Note: To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
Disk Reads	Number of disk reads per second on the catalog store, main store, and temporary store.
Disk Writes	Number of disk writes per second on the catalog store, main store, and temporary store.

See also

- *Viewing Overview Statistics* on page 325

- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346

Viewing Cache Statistics

Display the cache statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Caches**.
3. Select the tab for the required information.

Note: Hover the mouse pointer over any line or bar graph to display information for that graph.

Tab	Description
Cache size	Catalog cache – the megabyte allocation for the catalog cache, and the number of megabytes in use. Main cache – the megabyte allocation for the main cache, and the number of megabytes in use. Temporary cache – the megabyte allocation for the temporary cache, and the number of megabytes in use.
Cache reads	Number of cache reads per second for a period of time. The cache reads for the catalog, main, and temporary caches appear.

Tab	Description
Cache statistics	<p>Displays the cache statistics for the catalog, main, and temporary caches. Each cache type includes statistics for:</p> <p>Size (mb) – total size of the cache, in megabytes.</p> <p>In use (%) – percentage of the cache being used.</p> <p>Reads (per second) – number of cache reads per second.</p> <p>Hits (per second) – number of hits, per second, to the the catalog, main, and temporary caches.</p> <p>Dirty pages (%) – percentage of pages in the catalog, main, and temporary caches where data has been modified and stored in the buffer cache and has not yet been written to disk.</p> <p>Pinned – number of pinned catalog, main, and temporary cache pages.</p> <p>Pinned (%) – percentage of the catalog, main, and temporary chaches pinned.</p>

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346
- *Viewing Multiplex Cache Statistics* on page 377

Viewing Table Version Statistics

Display the table version statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Table Versions**.

Note: To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Area	Description
Statistics	<p>Number of committed versions – the number of table versions in the server.</p> <p>Total version space used (MB) – total space consumed by all the table versions.</p> <p>Oldest version ID – the oldest version identifier on the server.</p> <p>Number of active versions – total number of active write table versions on the server.</p> <p>Total active version space created (MB) – amount of data created by active write transactions.</p> <p>Total active version space to be destroyed (MB) – amount of data destroyed by active write transactions. If these transactions commit, the destroyed data becomes an old version and is eventually dropped. If the transactions roll back, the created data is released.</p>
Table versions	<p>Version ID – the table version identifier.</p> <p>Server name – the name of the server.</p> <p>Connection ID – the connection ID using this table version.</p> <p>MinKBRelease – the minimum amount of space returned once this version is no longer in use.</p> <p>MaxKBRelease – the maximum amount of space returned once this version is no longer in use.</p> <p>WasReported – indicates whether the server has received usage information for this version.</p>

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332

- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346

Viewing Operations and Requests Statistics

Display the operation and request statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Operations & Requests**.

Note: To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
Operations	<p>Total operations – the total number of IQ operations of any type.</p> <p>Active operations – the number of active IQ operations.</p> <p>Waiting operations – the number of IQ operations waiting for the resource governor.</p>
Requests	<p>Requests – the number of times per second the server has been accessed to handle a new request or continue processing an existing request.</p> <p>Active requests – the number of active requests.</p> <p>Unscheduled requests – the number of requests that are currently in the queue, waiting for an available server thread.</p>

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334

- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346

Viewing Network Statistics

Display the network statistics for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Network**.
3. Select the tab for the required information.

Note: To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
Network usage	Bytes received – amount of data, in bytes, received by the server. Bytes received uncompressed – amount of uncompressed data, in bytes, received by the server. Bytes sent – amount of data, in bytes, sent by the server. Bytes sent uncompressed – amount of uncompressed data, in bytes, sent by the server. Free communication buffers – number of free communication buffers. Total communication buffers – total number of communication buffers.
Data transfer history	Displays the amount of data, in kilobytes, sent and received by the server over time.
Buffer usage	Shows the total number of communication buffers, and a graph displaying the number of used and free communication buffers.

See also

- *Viewing Overview Statistics* on page 325

- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346

Viewing Table Page Usage Details

Display page usage details of tables or materialized views for the selected SAP Sybase IQ server. Table Page Usage only applies to system tables in the system store (IQ catalog store).

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Table Pages**.
3. From the **Tables** list, select the table or materialized view you want usage details about.

Note: To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Area	Description
Tables	<p>Name – the name of the table or materialized view.</p> <p>Owner – the user with owner privileges for the table or materialized view.</p> <p>Type – the type of table or materialized view.</p> <p>Table Pages – the number of pages in the table or materialized view.</p> <p>Table Pages Used Percentage – the percentage of used pages.</p> <p>Index Pages – the number of pages in the index of the table or materialized view.</p> <p>Index Pages Used Percentage – the percentage of used index pages.</p> <p>File Used Percentage – the percentage of the file that is used.</p>

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Lock Details* on page 343
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346

Viewing Table Lock Details

Use the Sybase Control Center node-level monitor view to display details of locked tables, views or materialized views for the selected SAP Sybase IQ server.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Table Locks**.
3. From the **Table Locks** list, select the lock you want details about by highlighting the locking connection, name of user holding the lock or locked table.

Note: To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Area	Description
Table Lock Details	<p>Connection ID – identifies the locking connection.</p> <p>Table Type – indicates whether the lock is on a table or materialized view.</p> <p>Table Owner – identifies the owner of the locked table or materialized view.</p> <p>Index ID – identifies the index of the locked table or materialized view.</p> <p>Lock Class – indicates the classification as Schema, Row, Table, or Position..</p> <p>Lock Duration – indicates the duration as Transaction, Position, or Connection.</p> <p>Lock Type – indicates the type (dependant on the lock class).</p> <p>Row ID – identifies the row with an 8-byte row identifier or NULL.</p>

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334

- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Deadlock Details* on page 344
- *Viewing Monitor Settings Details* on page 346

Viewing Deadlock Details

Write locks maintain the reliability of information by preventing concurrent access to rows or tables by more than one transaction. Transaction blocking and snapshot versioning manage statements until a lock becomes available. However, deadlock can occur when a set of transactions arrive at a state where none of them can proceed. Sybase Control Center allows you to view deadlock details, and to specify how these details are displayed.

Prerequisites

Database Version	View Deadlock Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

If you do not have the required pre-requisites, the deadlock details will be read-only.

Task

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Deadlocks**.
3. From the list, select the deadlock you want details about.

Area	Description
Waiter	The resource (server) that the proxy table will be created on.
Waiter Connection ID	The defined remote server containing the remote object to be represented by the proxy table.
Owner Connection ID	The defined local user that will own the proxy table.

4. View the deadlock details.

Area	Description
Snapshot ID	Identifies the snapshot version managing the transaction.
Snapshot Time	Indicates when the snapshot was created.
Object ID	Identifies the table, materialized view or other object causing the deadlock.
Record ID	Identifies the record causing the deadlock, if one exists.
Table Name	Indicates the name of the deadlocked table in owner.table format
Is Victim	A boolean indicator showing whether this connection was the victim of the deadlock
Primary Key	Indicates the primary key for the deadlocked table.
Rollback Operation Count	The number of times the rollback command has been executed to resolve the deadlock.
SQL Statement	Displays the SQL statement which caused the deadlock.

5. (Optional) If you have the appropriate authority, select **Clear Deadlock Information** to remove all items from the list.
6. (Optional) If you have the appropriate authority, select **Deadlock Settings** to modify how deadlock details are collected and displayed.
 - a) Specify whether to create a list of deadlocks with the **Collect information** check-box.
 - b) Specify whether to include the causal SQL statements in the list of deadlocks with the **SQL statement** check-box.

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336

- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343
- *Viewing Monitor Settings Details* on page 346

Viewing Monitor Settings Details

You can control the rate at which data on monitor screens and charts is refreshed, the amount of time covered by charts.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Node**.
2. In the left pane of the IQ Node Level Monitor view, select **Settings**.

Setting	Description
Screen re-fresh interval (Seconds)	Enter the number of seconds between refreshes. You can also use the up and down arrows to select the appropriate number of seconds. The default is 30 seconds.
Chart Trend Period	<p>Enter the number of minutes of data to appear in charts. The minimum number of minutes is 5, and the maximum number is 999999999. The default is 30 minutes.</p> <p>Since data is added to a chart only when it is open, a chart contains data starting from when you opened it. Each refresh interval adds new data to the end of the graph. A chart trend period of 30 minutes shows the statistics trend over the last 30 minutes, even if the view has been open longer than 30 minutes.</p>

See also

- *Viewing Overview Statistics* on page 325
- *Viewing All Statistics* on page 328
- *Viewing Engine Statistics* on page 328
- *Viewing Connection Statistics* on page 330
- *Viewing Transaction Statistics* on page 332
- *Viewing Dbspaces Statistics* on page 334
- *Viewing Store I/O Statistics* on page 335
- *Viewing Cache Statistics* on page 336
- *Viewing Table Version Statistics* on page 337
- *Viewing Operations and Requests Statistics* on page 339
- *Viewing Network Statistics* on page 340
- *Viewing Table Page Usage Details* on page 341
- *Viewing Table Lock Details* on page 343

- *Viewing Deadlock Details* on page 344

Administer Simplex Servers

Start, or stop a server, view properties, change server configuration, or generate administration scripts.

See also

- *Converting a Simplex Server to Multiplex* on page 356

Editing the Simplex Server Configuration File

Change simplex server configuration settings including administrative, memory, connection, and debugging settings.

Prerequisites

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The simplex server's SCC agent is registered, authenticated, and running.

Task

Editing the configuration file edits the `params.cfg` file located in the database directory for the server. You cannot edit a custom configuration file. If `params.cfg` does not exist, the Sybase Control Center agent automatically generates it when you adjust any configuration values and click **OK** or **Apply**.

Important: The Start Server wizard starts the server using the `params.cfg` file. You cannot start a server using a custom configuration file with a different name.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers**.
3. Select the IQ server from the right pane and either:
 - Click the drop-down arrow to the right of the name and select **Edit Configuration File**, or,
 - From the Administration Console menu bar select **Resource > Edit Configuration File**.

The Config file editor view appears.

4. Adjust the configuration values.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.

Area	Description
Admin	<p>Disable triggers – Disable firing of triggers.</p> <p>Checkpoint timeout period – Set the maximum length of time, in minutes, that the database server runs without doing a checkpoint.</p> <p>Maximum recovery time – Set the maximum length of time, in minutes, that the database server takes to recover from system failure.</p> <p>Start database permission – Specify permission required to start the database: "dba", "all" or "none".</p> <p>Stop database permission Specify permission required to stop the database: "dba", "all" or "none".</p> <p>Load/unload permission – Set LOAD/UNLOAD permission to "dba", "all" or "none".</p> <p>Utility permission – Set utility commands (e.g., DROP DATABASE) permission to "utility_db", "dba", "all" or "none".</p>

Area	Description
Memory	<p>Display cache sizing statistics – Displays cache size changes.</p> <p>Disable automatic cache resizing – Enforces a static cache size. Disables automatic cache resizing.</p> <p>Initial cache size – Sets the initial memory reserved for caching database pages and other server information. The size is the amount of memory. Select Kilobytes, Megabytes, Gigabytes. Select % to specify a percentage either of the physical system memory, or of the maximum non-AWE cache size, whichever is lower.</p> <p>Minimum cache size – Sets a minimum cache size as a lower limit to automatic cache resizing. The size is the amount of memory, in bytes. Select Kilobytes, Megabytes, Gigabytes. Select % to specify a percentage either of the physical system memory, or of the maximum non-AWE cache size, whichever is lower.</p> <p>Maximum cache size – Sets a maximum cache size, as a limit to automatic cache growth. The size is the amount of memory, in bytes. Select Kilobytes, Megabytes, Gigabytes. Select % to specify a percentage either of the physical system memory, or of the maximum non-AWE cache size, whichever is lower.</p> <p>Engine thread stack size – Sets server thread stack size. The size is the amount of memory, in bytes. Select Kilobytes or Megabytes.</p> <p>Number of engine threads – Sets the number of execution threads used for the catalog store and connectivity while running with multiple users. Recommended value is 1.5 times the maximum number of concurrent connections to the server; minimum of 25.</p> <p>Number of concurrent OS threads – Sets maximum number of physical processors to use (up to licensed maximum).</p> <p>External DLL thread stack size – Sets the stack size for threads running external functions, in bytes. The default is 32 KB.</p> <p>Maximum page size – Sets the maximum page size in KB.</p>

Area	Description
Connections	<p>Shutdown after last database closes – Automatically shut down after the last database is closed.</p> <p>Encrypt communication messages – Enable packet encryption on the network server.</p> <p>Enable client-server character translation – Character set translation is turned on by default. There is a performance cost associated with character set translation. If you can set up an environment such that no character set translation is required, then you do not have to pay this cost, and your setup is simpler to maintain.</p> <p>Maximum connections – Specifies the maximum number of concurrent user connections.</p> <p>Communication packet size – Specifies a maximum packet size. If you want to send small amounts of data over the network, keep the default network packet size small. The default is 512 bytes.</p> <p>Idle time before disconnect – Set the amount of client idle time before the connection is terminated. If a client runs for the idle timeout period without submitting a request, the connection is severed.</p> <p>Liveness timeout – A liveness packet is sent across a client/server to confirm that a connection is intact. If the client runs for the liveness timeout period without detecting a liveness packet, the communication will be severed. This parameter works only with network server and TCP/IP communications protocols. The default is 120 seconds.</p> <p>Quitting time – Lets you specify a time when the database server is to shut down.</p> <p>Broadcast level – Specifies how the server reacts to broadcasts. (Ignore All) causes the server not to start up any UDP broadcast listeners. (dblocate) causes the server to not respond to broadcasts from dblocate, while leaving connection logic unaffected.</p>
Database	<p>Set database read-only – Forces all databases that start on the database server to be read-only. No changes to the databases are allowed: the database server doesn't modify the database files or transaction log files.</p> <p>Truncate xact log after checkpoint – Causes the transaction log to be truncated after each checkpoint for all databases.</p>

Area	Description
Debug	<p>Generate debug information – Display debugging information.</p> <p>Remember last statement on each connection – Instruct the database server to capture the most recently prepared SQL statement for each connection to a database on the server.</p> <p>Debug level – Enables request-level logging of operations.</p> <p>Debug output file name – Redirects HTTP Web service client procedure debug log to a file.</p> <p>Max output file size – Specify maximum size of file for server request logging.</p>

Area	Description
IQ	<p>Number of CPUs IQ can use – Specifies the number of CPUs available to IQ, overriding the physical number of CPUs for resource planning purposes. The value defaults to the total number of CPUs, but the range of available values is 1 – 128.</p> <p>Number of threads – Sets the number of execution threads that will be used for the catalog store and connectivity while running with multiple users. This parameter applies to all operating systems and servers. Each connection uses a thread for each request, and when the request is completed, the thread is returned to the pool for use by other connections. As no connection can have more than one request in progress at one time, no connection uses more than one thread at a time.</p> <p>Thread stack size – Specifies the stack size, in KB, for server execution threads running either in the background or as part of a thread team assisting the main server connection thread. The default is 512KB on 64-bit platforms, and 200KB on 32-bit platforms.</p> <p>Wired memory pool size – Pool of wired memory on HP and Sun UNIX systems. This memory is locked down so it cannot be paged by the operating system. Specify the memory size, in MB. Use this switch only if you have enough memory to dedicate for this purpose. Otherwise, you may cause serious performance degradation.</p> <p>Main buffer cache size – Specifies the main IQ store cache size in MB. Always specify the value for the size, but no units of measurement; for example specify 32 instead of 32MB.</p> <p>Temporary buffer cache size – Specifies IQ temporary store cache size in MB. Always specify the value for the size, but no units of measurement; for example specify 32 instead of 32MB.</p> <p>Number of concurrent queries – The number of concurrent queries is not the same as the number of connections. This setting can help SAP Sybase IQ optimize paging of buffer data out to disk and avoid overcommitting memory. The default value of this switch is equal to 2 times the number of CPUs on your machine, plus 10. You may find that another value, such as 2 times the number of CPUs plus 4, provides better throughput, especially when large numbers of users are connected.</p> <p>Number of partitions for buffer cache – Specifies the number of partitions in the IQ main and temp buffer caches. Must be a power of 2. Allowed values are: 0 (default), 1, 2, 4, 8, 16, 32, 64. By default, IQ</p>

Area	Description
	<p>computes the number of partitions automatically as <code>number_of_cpus/8</code>, rounded to the nearest power of 2, up to a maximum of 64. You may be able to improve performance by adjusting the number of cache partitions.</p> <p>Force recovery on database – Open database in forced recovery mode.</p>
Misc	<p>Quiet mode – Runs Interactive SQL in quiet mode.</p> <p>Run as a daemon – Using this option lets you run the server so that it continues running after the current user session ends.</p> <p>Use buffered disk I/O – Uses buffered disk I/O [Windows, UNIX].</p> <p>Syslog facility ID – Syslog facility ID. The default is user. Either none, user, daemon, local0,...,local7).</p> <p>Output message file name – Filename for copy of message window. File is truncated first.</p> <p>Output message file size – Appends .old to the log file name and starts a new file with the original name when log reaches the specified size.</p> <p>Touch temporary file timer – (UNIX servers) Causes the server to touch catalog store temporary files at intervals specified in minutes.</p> <p>User specified – Enables advanced users to specify configuration options not shown in the Config file editor window. Enter multiple parameters using the space character as a separator.</p>

5. Click **OK**.

See also

- *Starting a Simplex Server* on page 354
- *Stopping a Simplex Server* on page 355
- *Converting a Simplex Server to Multiplex* on page 356
- *Generating an Administration Script for a Simplex Server* on page 358
- *Viewing or Modifying Simplex Server Properties* on page 359
- *Simplex Privilege Summary* on page 364
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Starting a Simplex Server

Start a simplex server.

Prerequisites

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The simplex server's SCC agent is registered, authenticated, and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane of the Administration Console, select **IQ Servers**.
3. Select one or more IQ servers from the right pane and either:
 - Click the drop-down arrow to the right of the name and select **Start Server**, or,
 - From the Administration Console menu bar select **Resource > Start Server**.

Tip: Use **Shift-click** or **Control-click** to select multiple IQ servers.

4. Click **Finish**.

See also

- *Editing the Simplex Server Configuration File* on page 347
- *Stopping a Simplex Server* on page 355
- *Converting a Simplex Server to Multiplex* on page 356
- *Generating an Administration Script for a Simplex Server* on page 358
- *Viewing or Modifying Simplex Server Properties* on page 359
- *Simplex Privilege Summary* on page 364
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Stopping a Simplex Server

Stop a simplex server.

Prerequisites

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane of the Administration Console, select **IQ Servers**.
3. Select one or more IQ servers from the right pane and either:
 - Click the drop-down arrow to the right of the name and select **Stop Server**, or,
 - From the Administration Console menu bar select **Resource > Stop Server**.

Tip: Use **Shift-click** or **Control-click** to select multiple IQ servers.

4. Click **Finish**.

See also

- *Editing the Simplex Server Configuration File* on page 347
- *Starting a Simplex Server* on page 354
- *Converting a Simplex Server to Multiplex* on page 356
- *Generating an Administration Script for a Simplex Server* on page 358
- *Viewing or Modifying Simplex Server Properties* on page 359
- *Simplex Privilege Summary* on page 364
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Converting a Simplex Server to Multiplex

Add a secondary server to a simplex to convert the simplex into a multiplex.

Prerequisites

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane of the Administration Console, select **IQ Servers**.
3. Select the IQ server from the right pane and either:
 - Click the arrow to the right of the name and select **Add Secondary Servers**, or
 - From the Administration Console menu bar, select **Resource > Add Secondary Servers**

The Add Secondary Servers wizard appears.

4. On the Server Definitions page, enter a name in the **Multiplex Name** field.
5. Click **Add** and specify:

Option	Description
Server name	Secondary server name.
Host	The host name and port number for the new secondary server.
Database path	The path to the database file.
SCC agent port	Port number for the Sybase Control Center agent.

Option	Description
SCC agent user	User ID for the Sybase Control Center agent.
SCC agent password	Password for the Sybase Control Center agent.
Public host/port pairs	Host/port pairs in the format host1:port1,host2:port2 , and so on.
Private host/port pairs	Host/port pairs in the format host1:port1,host2:port2 , and so on.
Role	Reader or writer.
Status	Included or excluded.
Local temp dbspace path	Temporary store path.
Local temp dbspace size (MB)	Size, in megabytes, of the temporary IQ store. 0 if you select a raw device.
Local temp dbspace reserve (MB)	The amount of space, in megabytes, to reserve for future expansion in the temporary IQ store.
Raw device	Indicates a raw disk.

6. Click **OK**.
7. (Optional) Import server definitions from a CSV file.
 - a) On the Node Definitions page of the wizard, click **Import** and specify:

Option	Description
File Name	File name of the CSV file containing delimited list of server definitions.
Browse	Opens a window where you locate the CSV file.
Field Delimiter	The default field delimiter is a vertical bar " ". If your CSV file uses a different field delimiter, enter it in this field.

- b) Click **OK**.
8. (Optional) Export your existing server definitions to a CSV file for safekeeping:
 - a) On the Node Definitions page of the wizard, click **Export** and specify:

Option	Description
--------	-------------

Option	Description
Field Delimiter	The default field delimiter is a vertical bar " ". You can specify a different field delimiter.

b) Click **OK**.

9. Click **Execute**.

If Sybase Control Center continues to display the converted multiplex server as a simplex, re-authenticate the simplex resource to force SCC to update its display.

See also

- *Editing the Simplex Server Configuration File* on page 347
- *Starting a Simplex Server* on page 354
- *Stopping a Simplex Server* on page 355
- *Generating an Administration Script for a Simplex Server* on page 358
- *Viewing or Modifying Simplex Server Properties* on page 359
- *Simplex Privilege Summary* on page 364
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating an Administration Script for a Simplex Server

Generate the configuration file and scripts for starting, stopping, and synchronizing a simplex server.

Prerequisites

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The simplex server's SCC agent is registered, authenticated, and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane of the Administration Console, select **IQ Servers**.
3. Select one or more IQ servers from the right pane and either:

- Click the drop-down arrow to the right of the name and select **Generate Administration Scripts**, or,
- From the Administration Console menu bar select **Resource > Generate Administration Scripts**.

Tip: Use **Shift-click** or **Control-click** to select multiple IQ servers.

The following scripts are generated:

- `params.cfg`
- `start_server.sh / start_server.bat`
- `stop_server.sh / stop_server.bat`

Note: The `stop_server` script requires your username and password. For example:
`stop_server.bat myname mypwd`

See also

- *Editing the Simplex Server Configuration File* on page 347
- *Starting a Simplex Server* on page 354
- *Stopping a Simplex Server* on page 355
- *Converting a Simplex Server to Multiplex* on page 356
- *Viewing or Modifying Simplex Server Properties* on page 359
- *Simplex Privilege Summary* on page 364
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Simplex Server Properties

View or change general, configuration, and agent information, and options and values of properties for the selected simplex server.

Prerequisites

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	View any simplex property page – None required. Modify any simplex property – Requires DBA authority.

Database Version	Simplex Privileges
SAP Sybase IQ 16.0	<p>View any simplex property page – None required.</p> <p>Modify any property on the Configuration or Options property page – Requires SERVER OPERATOR system privilege.</p> <p>Modify any property on the Request Logging property page – Requires one of:</p> <ul style="list-style-type: none"> MANAGE PROFILING system privileges. SERVER OPERATOR system privileges.

- The SAP Sybase IQ resource is authenticated and running.
- The simplex server's SCC agent is registered, authenticated, and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane of the Administration Console, select **IQ Servers**.
3. Select the IQ server in the right pane and either:
 - Click the drop-down arrow to the right of the name and select **Properties**, or,
 - From the Administration Console menu bar, select **Resource > Properties**.

The Server Properties view appears.

4. View or modify the server properties.
 - Configuration changes may take several minutes to complete.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode..

Area	Description
General (Read-only)	<p>Server name – Name of the server.</p> <p>Host – Host name where the server is running.</p> <p>Port – Port where the server is running.</p> <p>Database – Database name.</p> <p>Server version – Server version number.</p> <p>Platform – Platform the server is running on.</p> <p>Platform version – Version of the operating system where the server is running.</p> <p>Type – Server type: Single Server.</p>
Configuration	<p>Server name – Name of the server.</p> <p>Host – Host name where the server is running.</p> <p>Port – Port where the server is running.</p> <p>Database file path – Location of the .db file.</p>

Area	Description
Agent (Read-only)	<p>Agent registered – Indicates if the Sybase Control Center agent is registered: true or false.</p> <p>Agent authenticated – Indicates if the Sybase Control Center agent is authenticated: true or false.</p> <p>Agent status – Status of the Sybase Control Center agent: Running, Stopped, or Unknown.</p> <p>Agent host – Name of the host machine where the Sybase Control Center agent is running.</p> <p>Agent port – Port number on the host machine where the Sybase Control Center agent is running.</p> <p>Agent user – User name for authentication of the agent. Default is <i>uafadmin</i>.</p> <p>Agent process owner – The user name that owns the agent process.</p> <p>Agent home – The home directory of the Sybase Control Center agent.</p> <p>Agent version – The version of the Sybase Control Center agent.</p> <p>SCC agent plugin version – The agent plugin version of the Sybase Control Center agent.</p> <p>IQ directory – Installation directory of the IQ server with which the Sybase Control Center agent is associated.</p> <p>IQ version – Version of the IQ server with which the Sybase Control Center agent is associated.</p>
Server Properties (Read-only)	<p>Properties – The name, value, and description of all server properties.</p>

Area	Description
Request Logging	<p>Enable request logging – Check to enable request logging.</p> <p>All connections to this server – Check to log requests from all connections to the server.</p> <p>All connections to the following database – Specify the name of a database to log requests to all connections.</p> <p>The following connections – Specify the connections to log.</p> <p>Select type of requests to log – Check the type of requests to log:</p> <ul style="list-style-type: none"> • All • Include host variables • Triggers • Connections blocked from proceeding • SQL • Procedures • Plan <p>Log file name – Specify the pathname of the log file.</p> <p>Maximum log file size – Specify the maximum size of the log file.</p> <p>Maximum number of log files – Specify the maximum number of log files.</p> <p>Overwrite the request log file if it already exists – Check to overwrite an existing log file.</p>
Options	<p>Current time – The current time.</p> <p>Refresh – Click Refresh to update the current time.</p> <p>Quitting time – Enter a time for the database server to shut down. Use the same format as the current time: YYYY-MM-DD HH:NN:SS.SS</p> <p>Disable new connections – Prevent other users from connecting to the database. This may be useful for some maintenance operations.</p> <p>Remember last statement – Instruct the database server to capture the most recently prepared SQL statement for each connection to a database on the server.</p>

5. Click **OK**.

See also

- *Editing the Simplex Server Configuration File* on page 347

- *Starting a Simplex Server* on page 354
- *Stopping a Simplex Server* on page 355
- *Converting a Simplex Server to Multiplex* on page 356
- *Generating an Administration Script for a Simplex Server* on page 358
- *Simplex Privilege Summary* on page 364
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Simplex Privilege Summary

A list of the system privileges and object permissions required to complete the various simplex server tasks

Editing the Simplex Server Configuration File

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Starting or Stopping a Simplex Server

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

Converting a Simplex Server to Multiplex

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Generating an Administration Script for a Simplex Server

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.

Database Version	Simplex Privileges
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Simplex Server Properties

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	View any simplex property page – None required. Modify any simplex property – Requires DBA authority.
SAP Sybase IQ 16.0	View any simplex property page – None required. Modify any property on the Configuration or Options property page – Requires SERVER OPERATOR system privilege. Modify any property on the Request Logging property page – Requires one of: <ul style="list-style-type: none"> MANAGE PROFILING system privileges. SERVER OPERATOR system privileges.

See also

- *Editing the Simplex Server Configuration File* on page 347
- *Starting a Simplex Server* on page 354
- *Stopping a Simplex Server* on page 355
- *Converting a Simplex Server to Multiplex* on page 356
- *Generating an Administration Script for a Simplex Server* on page 358
- *Viewing or Modifying Simplex Server Properties* on page 359

Multiplex Servers

Manage and monitor multiplex servers in the SAP Sybase IQ environment.

Monitor Multiplex Servers

Statistics allow you to monitor the availability and performance of multiplex servers.

Note: Your login policy governs server access. Use a login ID with access to the SERVER logical server to manage a multiplex. SERVER logical server context requires the ACCESS SERVER LS system privilege. In the *SAP Sybase IQ* documentation, see *SAP Sybase IQ Administration: Multiplex* for details on login policies and logical server configuration.

Viewing Multiplex Overview Statistics

Display the overall health of the SAP Sybase IQ multiplex environment.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Overview**.
3. Select the tab for the required information.

Note: Click a column header to sort the data by that column.

To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
Multiplex tab > Servers	<p>Server – name of the server.</p> <p>Host – host name where the server is running.</p> <p>Port – port number where the server is running.</p> <p>State – current state of the server. Valid states include:</p> <ul style="list-style-type: none"> • Unknown • Stopped • Running <p>Role – role the server plays in the multiplex configuration. Roles include:</p> <ul style="list-style-type: none"> • Coordinator • Reader • Writer <p>Status – current status of the server in the multiplex. Valid states include:</p> <ul style="list-style-type: none"> • Included • Excluded
Multiplex tab > CPU History	Percentage of total CPU usage over a period of time for each server. The legend below the chart identifies the colored line associated with each server.
Multiplex tab > IQ Memory	Allocation of the IQ memory between the main cache and temporary cache for each server in the multiplex.

Area	Description
Disk Usage tab	Available and used space for the main store and temporary store on each server in the multiplex.
Version Usage tab > Statistics	<p>Number of committed versions – the number of table versions in the servers.</p> <p>Total version space used (MB) – total space consumed by all the table versions.</p> <p>Oldest version ID – the oldest table version identifier on the server.</p> <p>Number of active versions – total number of active write table versions on the servers.</p> <p>Total active version space created (MB) – amount of data created by active write transactions.</p> <p>Total active version space to be destroyed (MB) – amount of data destroyed by active write transactions. If these transactions commit, the destroyed data becomes an old version and is eventually dropped. If the transactions roll back, the created data is released.</p>
Version Usage tab > Multiplex Version Usage	<p>Version ID – the table version identifier.</p> <p>Server name – the name of the server where the table version exists.</p> <p>Connection ID – the connection ID using this table version.</p> <p>WasReported – indicates whether the server has received usage information for this table version.</p> <p>MinKBRelease – the minimum amount of space returned once this table version is no longer in use.</p> <p>MaxKBRelease – the maximum amount of space returned once this table version is no longer in use.</p>
Alerts	Any alerts for the selected multiplex. While the monitor is open, alerts are displayed as they are created.

See also

- *Viewing Multiplex Topology Statistics* on page 368
- *Viewing Multiplex Server Statistics* on page 372
- *Viewing Multiplex Connection Statistics* on page 374
- *Viewing Multiplex Transaction Statistics* on page 375
- *Viewing Multiplex Dbspace Statistics* on page 376
- *Viewing Multiplex Cache Statistics* on page 377
- *Viewing Multiplex Monitor Settings Details* on page 378
- *Viewing Overview Statistics* on page 325

Viewing Multiplex Topology Statistics

Display the topology view of the SAP Sybase IQ multiplex.

The topology view represents the entire multiplex grid environment, which consists of nodes and links. A node represents a multiplex server, while a link represents the connection between two multiplex nodes. Only one coordinator node appears, and links exist only between the coordinator node and a secondary node. There are no links between two secondary nodes.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Topology**.
3. To modify the layout of the topology view, click **View Controls**.

Layout options include:

- **Autofit** – rearranges the nodes to ensure all nodes are visible.
 - **Zoom** – increases or decreases the size of the view.
 - **Reset** – restores the topology view to the default layout.
4. To view a list of the all nodes in the multiplex, and a list of the connections between the coordinator node and its secondary nodes within the multiplex, click **Details**.
 5. To monitor a single node within the multiplex, right-click the node in the topology view and select **Monitor Node**.

When monitoring a single node from the topology screen, the IQ Node Level Monitor is displayed, and the node is registered as a single node resource and appears in the Perspective Resources view.

See also

- *Viewing Multiplex Overview Statistics* on page 366
- *Viewing Multiplex Server Statistics* on page 372
- *Viewing Multiplex Connection Statistics* on page 374
- *Viewing Multiplex Transaction Statistics* on page 375
- *Viewing Multiplex Dbspace Statistics* on page 376
- *Viewing Multiplex Cache Statistics* on page 377
- *Viewing Multiplex Monitor Settings Details* on page 378

Displaying the Properties of a Multiplex Node

View the server information for a single node in the multiplex environment.

1. In the Perspective Resources window, select the resource and select **Resource > Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Topology**.

3. Right-click the node and select **Properties**.

The Server Properties dialog includes:

Area	Description
General	<p>Server name – name of the server.</p> <p>Host – host name where the server is running.</p> <p>Port – port number where the server is running.</p> <p>State – current state of the server. Valid states include:</p> <ul style="list-style-type: none"> • Unknown • Stopped • Running <p>INC state – state of the internode communication between the secondary node and the coordinator. Valid values include:</p> <ul style="list-style-type: none"> • Active • Timed out • N/A (not available) • Unknown <hr/> <p>Note: When viewing the properties of the coordinator node, the INC state always displays N/A.</p> <hr/> <p>Role – role of the server within the multiplex. Valid roles include:</p> <ul style="list-style-type: none"> • Coordinator • Writer • Reader <p>Status – current status of the server. Valid statuses include:</p> <ul style="list-style-type: none"> • Included • Excluded <p>Database Path – location of the database file on the server.</p>
MIPC	<p>Node – Multiplex node name.</p> <p>Public Status – Current public status of each node. Status is set to “Not responding” if communication with that node fails.</p> <p>Private Status – Current private status of each node. Status is set to “Not configured” or “Not responding” if there is no Private TCP/IP configuration for that server.</p>

See also

- *Displaying Connection Properties* on page 370
- *Monitoring a Single Node in a Multiplex Server* on page 372

Displaying Connection Properties

View the details of the connection between the coordinator node and a secondary node.

1. In the Perspective Resources window, select the resource and select **Resource > Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Topology**.
3. Right-click the line between the coordinator node and the secondary node and select **Properties**.

The internode communication properties dialog includes:

Area	Description
General	<p>Link – name of the linked coordinator node and secondary node.</p> <p>INC state – state of the internode communication between the secondary node and the coordinator. Valid values include:</p> <ul style="list-style-type: none"> • Active • Timed out • N/A (not available) • Unknown <p>Secondary server name – name of the secondary server.</p> <p>Heartbeat frequency – number of seconds between polls to ensure the secondary server is connected.</p> <p>Last successful heartbeat – date and time the last successful heartbeat transmission was received.</p> <p>Time not responding – amount of time since the first failed heartbeat request.</p> <p>Time until timeout – amount of time until the server connection times out and the secondary node becomes inactive.</p> <p>Liveness timeout – amount of time before the connection is terminated.</p> <p>Auto exclude timeout – amount of time before the secondary node is automatically excluded.</p> <p>Max connection pool size – maximum number of connections in the secondary node's pool of INC connections.</p> <p>Current connection pool size – current number of connections to the servercurrent number of connections in the secondary node's pool of INC connections.</p> <p>Number of idle connections – current number of unused INC connections from the secondary node to the coordinator.</p> <p>Number of connections in use – current number of INC connections in use from the secondary node to the coordinator.</p>

See also

- *Displaying the Properties of a Multiplex Node* on page 368
- *Monitoring a Single Node in a Multiplex Server* on page 372

Monitoring a Single Node in a Multiplex Server

Monitor the availability and performance of a single node in a multiplex server.

1. In the Perspective Resources window, select the resource and select **Resource > Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Topology**.
3. Right-click the node and select **Monitor Node**.
The IQ Node Level Monitor view for the node appears. For information on each statistic that can be monitored for the node, see *Sybase Control Center for SAP Sybase IQ > Administer and Monitor SAP Sybase IQ > Monitor Simplex Servers*.

See also

- *Displaying the Properties of a Multiplex Node* on page 368
- *Displaying Connection Properties* on page 370

Viewing Multiplex Server Statistics

Display the statistics for the servers in the SAP Sybase IQ multiplex.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Servers**.
3. In the Multiplex Servers area, select the server to display in the Server Details area.

Note: Click a column header to sort the data by that column.

To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Tab	Description
Multiplex Servers	<p>Server – name of the server.</p> <p>Host – host name where the server is running.</p> <p>Port – port number where the server is running.</p> <p>State – current state of the server. Valid states include:</p> <ul style="list-style-type: none"> • Unknown • Stopped • Running <p>Role – role of the server within the multiplex. Valid roles include:</p> <ul style="list-style-type: none"> • Coordinator • Writer • Reader <p>Status – current status of the server. Valid states include:</p> <ul style="list-style-type: none"> • Included • Excluded
Server Details	<p>Server name – name of the server.</p> <p>State – current state of the server. Valid states include:</p> <ul style="list-style-type: none"> • Unknown • Stopped • Running <p>Database – name of the IQ database.</p> <p>Database path – location of the database file on the server.</p> <p>Server version – version of the IQ server.</p> <p>Platform – operating system running on the host of the server.</p>

See also

- *Viewing Multiplex Overview Statistics* on page 366
- *Viewing Multiplex Topology Statistics* on page 368
- *Viewing Multiplex Connection Statistics* on page 374
- *Viewing Multiplex Transaction Statistics* on page 375
- *Viewing Multiplex Dbspace Statistics* on page 376
- *Viewing Multiplex Cache Statistics* on page 377
- *Viewing Multiplex Monitor Settings Details* on page 378

Viewing Multiplex Connection Statistics

Display the connection statistics for all servers in an SAP Sybase IQ multiplex.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Connections**.
3. To display a list of connections in the Multiplex Connections area, click the arrow beside the server name.
4. On the Active Connections tab, click the bar chart for a server to display the active connection details in a pie chart.

Note: To display the information in a chart or table in the full window, select the **Maximize** icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
Connections tab > Multiplex Connections	<p>Displays all users currently connected to each server, including:</p> <p>Server – the name of the server.</p> <p>User ID – the ID of the connected user.</p> <p>Connection ID – the ID of the connection.</p> <p>State – the current state of the selected connection. Possible states include:</p> <ul style="list-style-type: none"> • ACTIVE – the connection is live. • SUSPENDED – the connection and its corresponding transaction are suspended, probably due to hardware or communication failure. <p>Name – the name of the connection.</p> <p>Connection create time – the date and time the connection was established.</p> <p>Client IP address – the IP address of the client that made the connection.</p> <p>Connection or cursor – indicates a connection or an active cursor</p>

Area	Description
Connections tab > User Connections/Disconnections Per Minute	Displays the number of user connections and disconnections per minute for each server.
Active Connections tab	Displays a chart of the number of user, internode incoming, and other connections to the selected server.

See also

- *Viewing Multiplex Overview Statistics* on page 366
- *Viewing Multiplex Topology Statistics* on page 368
- *Viewing Multiplex Server Statistics* on page 372
- *Viewing Multiplex Transaction Statistics* on page 375
- *Viewing Multiplex Dbspace Statistics* on page 376
- *Viewing Multiplex Cache Statistics* on page 377
- *Viewing Multiplex Monitor Settings Details* on page 378
- *Viewing Connection Statistics* on page 330

Viewing Multiplex Transaction Statistics

Display transaction statistics for all servers in an SAP Sybase IQ multiplex.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Transactions**.
3. To display a list of transactions, click the arrow beside the server name.
4. On the Transaction Statistics tab, click the bar chart for a server to display the transaction details in a pie chart.

Note: To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
------	-------------

Area	Description
Transactions tab	<p>Server – the name of the server.</p> <p>Transaction ID – the unique identification number for the selected transaction.</p> <p>Version ID – the version identification number for the selected transaction.</p> <p>User ID – the user name of the user that started the selected transaction.</p> <p>State – the current state of the selected transaction. Possible states include:</p> <ul style="list-style-type: none"> • ACTIVE – the transaction is being processed. • COMMITTED – the transaction has completed processing. <p>Creation time – the date and time when the selected transaction was created.</p>
Transaction Statistics tab	Displays a chart of the number of transactions for each server in the multiplex. Selecting a server in the chart displays a pie chart of user and internode communications (identified on the chart as INC) transactions.

See also

- *Viewing Multiplex Overview Statistics* on page 366
- *Viewing Multiplex Topology Statistics* on page 368
- *Viewing Multiplex Server Statistics* on page 372
- *Viewing Multiplex Connection Statistics* on page 374
- *Viewing Multiplex Dbspace Statistics* on page 376
- *Viewing Multiplex Cache Statistics* on page 377
- *Viewing Multiplex Monitor Settings Details* on page 378
- *Viewing Transaction Statistics* on page 332

Viewing Multiplex Dbspace Statistics

View dbspace size and usage details for multiplex dbspaces, including shared temporary dbspaces.

1. In the Perspective Resources view, highlight the resource and select **Resource > Administration Console**.
2. In the left pane of the Administration Console view, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. In the Multiplex Servers tab, highlight a resource.
4. Hover the mouse pointer over the resource name, click the arrow, and select **Monitor**.
5. In the Launch Monitor view, click **Yes**.
6. In the left pane of the IQ Node Level Monitor view, select **Dbspaces**.
7. In the Dbspaces pane, highlight the dbspace name.

The Dbspace Details pane displays Dbspace size, and Percent available. The Size Details tab show a pie chart comparing Dbspace size in use to size available. The DB Files pane shows all the DB files that are part of highlighted Dbspace.

8. If multiple DB files appear in the DB Files pane, highlight the DB file to show its information in the DB File Details pane.

See also

- *Viewing Multiplex Overview Statistics* on page 366
- *Viewing Multiplex Topology Statistics* on page 368
- *Viewing Multiplex Server Statistics* on page 372
- *Viewing Multiplex Connection Statistics* on page 374
- *Viewing Multiplex Transaction Statistics* on page 375
- *Viewing Multiplex Cache Statistics* on page 377
- *Viewing Multiplex Monitor Settings Details* on page 378

Viewing Multiplex Cache Statistics

Display the cache statistics for all servers in an SAP Sybase IQ multiplex.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Caches**.
3. Select the tab for the cache type to show.

Each cache type tab provides a graph with colored lines for each selected server.

Note: To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Chart	Description
Cache Reads	Number of cache reads per second for a period of time. The cache reads for the catalog, main, and temporary caches appear. The legend at the right of the chart identifies the colored line associated with each server.
Cache Size	The megabyte allocation for the selected cache type on each server in the multiplex, and the number of megabytes in use.

See also

- *Viewing Multiplex Overview Statistics* on page 366
- *Viewing Multiplex Topology Statistics* on page 368
- *Viewing Multiplex Server Statistics* on page 372

- *Viewing Multiplex Connection Statistics* on page 374
- *Viewing Multiplex Transaction Statistics* on page 375
- *Viewing Multiplex Dbspace Statistics* on page 376
- *Viewing Multiplex Monitor Settings Details* on page 378
- *Viewing Cache Statistics* on page 336

Viewing Multiplex Monitor Settings Details

You can control the rate at which data on monitor screens and charts is refreshed, the amount of time covered by charts, and the multiplex nodes included in charts.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Multiplex**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Settings**.

Setting	Description
Screen refresh interval (Seconds)	Enter the number of seconds between refreshes. You can also use the up and down arrows to select the appropriate number of seconds. The default is 30 seconds.
Chart Trend Period	Enter the number of minutes of data to appear in charts. The minimum number of minutes is 5, and the maximum number is 999999999. The default is 30 minutes. Since data is added to a chart only when it is open, a chart contains data starting from when you opened it. Each refresh interval adds new data to the end of the graph. A chart trend period of 30 minutes shows the statistics trend over the last 30 minutes, even if the view has been open longer than 30 minutes.
Maximum Number of Nodes to Show in Chart	Enter the maximum number of nodes to include in any monitoring charts. The default is 10 nodes.
Select Nodes	Choose the nodes to include in the monitoring charts. You cannot select more than the maximum number of nodes.

See also

- *Viewing Multiplex Overview Statistics* on page 366
- *Viewing Multiplex Topology Statistics* on page 368
- *Viewing Multiplex Server Statistics* on page 372
- *Viewing Multiplex Connection Statistics* on page 374
- *Viewing Multiplex Transaction Statistics* on page 375
- *Viewing Multiplex Dbspace Statistics* on page 376
- *Viewing Multiplex Cache Statistics* on page 377

Administer Multiplex Servers

Change a multiplex server configuration, manage the coordinator, secondary and failover nodes, and configure logical servers, start and stop servers. Statistics let you monitor multiplex availability and performance.

Note: Your login policy governs server access. Use a login ID with access to the SERVER logical server to manage a multiplex. SERVER logical server context requires the ACCESS SERVER LS system privilege. In the *SAP Sybase IQ* documentation, see *SAP Sybase IQ Administration: Multiplex* for details on login policies and logical server configuration.

Editing the Multiplex Server Configuration File

Change multiplex server configuration settings including administrative, memory, connection, and debugging settings.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

Editing the configuration file edits the `params.cfg` file located in the database directory for the server. You cannot edit a custom configuration file. If `params.cfg` does not exist, the Sybase Control Center agent automatically generates it when you adjust any configuration values and click **OK** or **Apply**.

Important: The Start Server wizard starts the server using the `params.cfg` file. You cannot start a server using a custom configuration file with a different name.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select a multiplex server from the right pane and either:
 - Click the drop-down arrow to the right of the name and select **Edit Configuration File**, or,

- From the Administration Console menu bar select **Resource > Edit Configuration File**.

The Config file editor window appears.

4. Adjust the configuration values.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
Admin	<p>Disable triggers – Disable firing of triggers.</p> <p>Checkpoint timeout period – Set the maximum length of time, in minutes, that the database server runs without doing a checkpoint.</p> <p>Maximum recovery time – Set the maximum length of time, in minutes, that the database server takes to recover from system failure.</p> <p>Start database permission – Specify permission required to start the database: "dba", "all" or "none".</p> <p>Stop database permission Specify permission required to stop the database: "dba", "all" or "none".</p> <p>Load/unload permission – Set LOAD/UNLOAD permission to "dba", "all" or "none".</p> <p>Utility permission – Set utility commands (e.g., DROP DATABASE) permission to "utility_db", "dba", "all" or "none".</p>

Area	Description
Memory	<p>Display cache sizing statistics – Displays cache size changes.</p> <p>Disable automatic cache resizing – Enforces a static cache size. Disables automatic cache resizing.</p> <p>Initial cache size – Sets the initial memory reserved for caching database pages and other server information. The size is the amount of memory. Select Kilobytes, Megabytes, Gigabytes. Select % to specify a percentage either of the physical system memory, or of the maximum non-AWE cache size, whichever is lower.</p> <p>Minimum cache size – Sets a minimum cache size as a lower limit to automatic cache resizing. The size is the amount of memory, in bytes. Select Kilobytes, Megabytes, Gigabytes. Select % to specify a percentage either of the physical system memory, or of the maximum non-AWE cache size, whichever is lower.</p> <p>Maximum cache size – Sets a maximum cache size, as a limit to automatic cache growth. The size is the amount of memory, in bytes. Select Kilobytes, Megabytes, Gigabytes. Select % to specify a percentage either of the physical system memory, or of the maximum non-AWE cache size, whichever is lower.</p> <p>Engine thread stack size – Sets server thread stack size. The size is the amount of memory, in bytes. Select Kilobytes or Megabytes.</p> <p>Number of engine threads – Sets the number of execution threads used for the catalog store and connectivity while running with multiple users. Recommended value is 1.5 times the maximum number of concurrent connections to the server; minimum of 25.</p> <p>Number of concurrent OS threads – Sets maximum number of physical processors to use (up to licensed maximum).</p> <p>External DLL thread stack size – Sets the stack size for threads running external functions, in bytes. The default is 32 KB.</p> <p>Maximum page size – Sets the maximum page size in KB.</p>

Area	Description
Connections	<p>Shutdown after last database closes – Automatically shut down after the last database is closed.</p> <p>Encrypt communication messages – Enable packet encryption on the network server.</p> <p>Enable client-server character translation – Character set translation is turned on by default. There is a performance cost associated with character set translation. If you can set up an environment such that no character set translation is required, then you do not have to pay this cost, and your setup is simpler to maintain.</p> <p>Maximum connections – Specifies the maximum number of concurrent user connections.</p> <p>Communication packet size – Specifies a maximum packet size. If you want to send small amounts of data over the network, keep the default network packet size small. The default is 512 bytes.</p> <p>Idle time before disconnect – Set the amount of client idle time before the connection is terminated. If a client runs for the idle timeout period without submitting a request, the connection is severed.</p> <p>Liveness timeout – A liveness packet is sent across a client/server to confirm that a connection is intact. If the client runs for the liveness timeout period without detecting a liveness packet, the communication will be severed. This parameter works only with network server and TCP/IP communications protocols. The default is 120 seconds.</p> <p>Quitting time – Lets you specify a time when the database server is to shut down.</p> <p>Broadcast level – Specifies how the server reacts to broadcasts. (Ignore All) causes the server not to start up any UDP broadcast listeners. (dblocate) causes the server to not respond to broadcasts from dblocate, while leaving connection logic unaffected.</p>
Database	<p>Set database read-only – Forces all databases that start on the database server to be read-only. No changes to the databases are allowed: the database server doesn't modify the database files or transaction log files.</p> <p>Truncate xact log after checkpoint – Causes the transaction log to be truncated after each checkpoint for all databases.</p>

Area	Description
Debug	<p>Generate debug information – Display debugging information.</p> <p>Remember last statement on each connection – Instruct the database server to capture the most recently prepared SQL statement for each connection to a database on the server.</p> <p>Debug level – Enables request-level logging of operations.</p> <p>Debug output file name – Redirects HTTP Web service client procedure debug log to a file.</p> <p>Max output file size – Specify maximum size of file for server request logging.</p>

Area	Description
IQ	<p>Number of CPUs IQ can use – Specifies the number of CPUs available to IQ, overriding the physical number of CPUs for resource planning purposes. The value defaults to the total number of CPUs, but the range of available values is 1 – 128.</p> <p>Number of threads – Sets the number of execution threads that will be used for the catalog store and connectivity while running with multiple users. This parameter applies to all operating systems and servers. Each connection uses a thread for each request, and when the request is completed, the thread is returned to the pool for use by other connections. As no connection can have more than one request in progress at one time, no connection uses more than one thread at a time.</p> <p>Thread stack size – Specifies the stack size, in KB, for server execution threads running either in the background or as part of a thread team assisting the main server connection thread. The default is 512KB on 64-bit platforms, and 200KB on 32-bit platforms.</p> <p>Wired memory pool size – Pool of wired memory on HP and Sun UNIX systems. This memory is locked down so it cannot be paged by the operating system. Specify the memory size, in MB. Use this switch only if you have enough memory to dedicate for this purpose. Otherwise, you may cause serious performance degradation.</p> <p>Main buffer cache size – Specifies the main IQ store cache size in MB. Always specify the value for the size, but no units of measurement; for example specify 32 instead of 32MB.</p> <p>Temporary buffer cache size – Specifies IQ temporary store cache size in MB. Always specify the value for the size, but no units of measurement; for example specify 32 instead of 32MB.</p> <p>Number of concurrent queries – The number of concurrent queries is not the same as the number of connections. This setting can help SAP Sybase IQ optimize paging of buffer data out to disk and avoid overcommitting memory. The default value of this switch is equal to 2 times the number of CPUs on your machine, plus 10. You may find that another value, such as 2 times the number of CPUs plus 4, provides better throughput, especially when large numbers of users are connected.</p> <p>Number of partitions for buffer cache – Specifies the number of partitions in the IQ main and temp buffer caches. Must be a power of 2. Allowed values are: 0 (default), 1, 2, 4, 8, 16, 32, 64. By default, IQ</p>

Area	Description
	<p>computes the number of partitions automatically as <code>number_of_cpus/8</code>, rounded to the nearest power of 2, up to a maximum of 64. You may be able to improve performance by adjusting the number of cache partitions.</p> <p>Force recovery on database – Open database in forced recovery mode.</p>
Transport Layer Security	<p>Use Transport Layer Security – Secure communications between a client and the SAP Sybase IQ server or between an SAP Sybase IQ client and the database server. SAP Sybase IQ supports only the RSA encryption algorithm. Check this box to enable other components on this page.</p> <p>Identity file – Contains the server's public certificate, private key and, for certificates that are not self-signed, all the signing certificates, including the encryption certificate. The password for this certificate must be specified with the <code>Identity_Password</code> parameter.</p> <p>Private key password – Must match the password supplied during encryption certificate creation. There is no default password.</p>
Misc	<p>Quiet mode – Runs Interactive SQL in quiet mode.</p> <p>Run as a daemon – Using this option lets you run the server so that it continues running after the current user session ends.</p> <p>Use buffered disk I/O – Uses buffered disk I/O [Windows, UNIX].</p> <p>Syslog facility ID – Syslog facility ID. The default is user. Either none, user, daemon, local0,...,local7).</p> <p>Output message file name – Filename for copy of message window. File is truncated first.</p> <p>Output message file size – Appends .old to the log file name and starts a new file with the original name when log reaches the specified size.</p> <p>Touch temporary file timer – (UNIX servers) Causes the server to touch catalog store temporary files at intervals specified in minutes.</p> <p>User specified – Enables advanced users to specify configuration options not shown in the Config file editor window. Enter multiple parameters using the space character as a separator.</p>

5. Click **OK**.

See also

- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Starting a Multiplex Server

Start a multiplex node.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select one or more multiplex servers from the right pane and either:
 - Click the drop-down arrow to the right of the name and select **Start Server**, or,

- From the Administration Console menu bar select **Resource > Start Server**.

Tip: Use **Shift-click** or **Control-click** to select multiple multiplex servers.

4. Click **Finish**.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Stopping a Multiplex Server

Stop a multiplex node.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select one or more multiplex servers from the right pane and either:
 - Click the drop-down arrow to the right of the name and select **Stop Server**, or,
 - From the Administration Console menu bar select **Resource > Stop Server**.

Tip: Use **Shift-click** or **Control-click** to select multiple multiplex servers.

4. Click **Finish**.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Including an Excluded Secondary Server

Include a previously excluded secondary server when the excluded server's shutdown period is over.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • All of these authorities: <ul style="list-style-type: none"> • MULTIPLEX ADMIN authority, and • BACKUP authority.

Database Version	Multiplex Privileges
SAP Sybase IQ 16.0	<p>Requires all of:</p> <ul style="list-style-type: none"> • <code>MANAGE MULTIPLEX</code> system privilege. • <code>SERVER OPERATOR</code> system privilege. • <code>BACKUP DATABASE</code> system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- The server you are including must have Excluded status.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select one or more multiplex servers from the right pane and either:
 - Click the arrow to the right of the name and select **Include Server**, or
 - From the Administration Console menu bar select **Resource > Include Server**

Tip: Use **Shift-click** or **Control-click** to select multiple multiplex servers.

4. Click **Finish**.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279

- *Authenticating a Login Account for a Managed Resource* on page 282

Excluding a Secondary Server

To save disk space, exclude any secondary server that will be shut down for an extended period.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

Servers that are shut down are still included in the multiplex. For each included server, the coordinator uses disk space to preserve all old versions of IQ objects changed since the server was shut down. Excluding a server allows the coordinator to ignore it during version cleanup.

Note: You cannot exclude the designated failover server, or the coordinator. Excluding a running server shuts it down.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select one or more multiplex servers from the right pane and either:
 - Click the arrow to the right of the name and select **Exclude Server**, or
 - From the Administration Console menu bar, select **Resource > Exclude Server**

Tip: Use **Shift-click** or **Control-click** to select multiple multiplex servers.

4. Click **Finish**.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386

- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Synchronizing a Secondary Server

Synchronization updates a secondary server with respect to the coordinator.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires both SERVER OPERATOR and BACKUP DATABASE system privileges.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select one or more multiplex servers from the right pane and either:
 - Click the arrow to the right of the name and select **Synchronize Server**, or
 - From the Administration Console menu bar select **Resource > Synchronize Server**

Tip: Use **Shift-click** or **Control-click** to select multiple multiplex servers.

4. On the Synchronize Server window, click **Finish**.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Adding a Secondary Server

Add a secondary server to the multiplex server.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• All of these authorities:<ul style="list-style-type: none">• MULTIPLEX ADMIN authority.• SPACE ADMIN authority.• BACKUP authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none">• SERVER OPERATOR system privilege.• MANAGE MULTIPLEX system privilege.• MANAGE ANY DBSPACE system privilege.• BACKUP DATABASE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select a multiplex server from the right pane and either:
 - Click the arrow to the right of the name and select **Add Secondary Server**, or
 - From the Administration Console menu bar, select **Resource > Add Secondary Server**

The Add Secondary Servers wizard appears.

4. On the Server Definitions page, click **Add** and specify:

Option	Description
Server name	Secondary server name.
Host	The host name and port number for the new secondary server.
Database path	The path to the database file.
SCC agent port	Port number for the Sybase Control Center agent.
SCC agent user	User ID for the Sybase Control Center agent.
SCC agent password	Password for the Sybase Control Center agent.
Public host/port pairs	Host/port pairs in the format host1:port1,host2:port2 , and so on.
Private host/port pairs	Host/port pairs in the format host1:port1,host2:port2 , and so on.
Role	Reader or writer.
Status	Included or excluded.
Local temp dbspace path	Temporary store path.
Local temp dbspace size (MB)	Size, in megabytes, of the temporary IQ store. 0 if you select a raw device.

Option	Description
Local temp dbspace reserve (MB)	The amount of space, in megabytes, to reserve for future expansion in the temporary IQ store.
Raw device	Indicates a raw disk.

5. Click **OK**.
6. (Optional) Import server definitions from a CSV file:
 - a) On the Server Definitions page of the wizard, click **Import** and specify:

Option	Description
File Name	File name of the CSV file containing delimited list of server definitions.
Browse	Opens a window where you locate the CSV file.
Field Delimiter	The default field delimiter is a vertical bar " ". If your CSV file uses a different field delimiter, enter it in this field.

- b) Click **OK**.
7. (Optional) Export your existing server definitions to a CSV file for safekeeping.
 - a) On the Server Definitions page of the wizard, click **Export** and specify:

Option	Description
Field Delimiter	The default field delimiter is a vertical bar " ". You can specify a different field delimiter.

- b) Click **OK**.
8. Click **Next**.
9. On the Execution page of the wizard, click **Execute**.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402

- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Dropping a Secondary Server

Remove a secondary server from a multiplex server. You can drop the designated failover server only if it is the only secondary server in the multiplex.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • All of these authorities: <ul style="list-style-type: none"> • MULTIPLEX ADMIN authority. • SPACE ADMIN authority. • BACKUP authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none"> • MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select one or more multiplex servers the right pane and either:
 - Click the arrow to the right of the name and select **Drop Secondary Node**, or
 - From the Administration Console menu bar, select **Resource > Drop Secondary Node**

Tip: Use **Shift-click** or **Control-click** to select multiple multiplex servers.

4. (Optional) Select **Delete the database directory**. This cleans up the database directory by removing any files that belong to the server.

Warning! Use caution in selecting the option to delete files. If any of the files to be deleted are shared main files, data can be lost, and servers might not start correctly afterwards.

5. Click **Finish**.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Administration Scripts for Multiplex Nodes

Generate the configuration file and scripts for starting, stopping, and synchronizing multiplex servers.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select one or more multiplex servers from the right pane and either:
 - Click the drop-down arrow to the right of the name and select **Generate Administration Scripts**, or,
 - From the Administration Console menu bar select **Resource > Generate Administration Scripts**.

Tip: Use **Shift-click** or **Control-click** to select multiple multiplex servers.

4. Click **Finish** to generate these scripts:

Windows	UNIX or Linux
params.cfg	params.cfg
start_server.bat	start_server.sh
stop_server.bat	stop_server.sh
sync_server.bat	sync_server.sh

Note: The stop_server and sync_server scripts require your username and password. For example: stop_server.bat myname mypwd

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279

- *Authenticating a Login Account for a Managed Resource* on page 282

Converting a Simplex Server to Multiplex

Add a secondary server to a simplex to convert the simplex into a multiplex.

Prerequisites

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane of the Administration Console, select **IQ Servers**.
3. Select the IQ server from the right pane and either:
 - Click the arrow to the right of the name and select **Add Secondary Servers**, or
 - From the Administration Console menu bar, select **Resource > Add Secondary Servers**

The Add Secondary Servers wizard appears.

4. On the Server Definitions page, enter a name in the **Multiplex Name** field.
5. Click **Add** and specify:

Option	Description
Server name	Secondary server name.
Host	The host name and port number for the new secondary server.
Database path	The path to the database file.
SCC agent port	Port number for the Sybase Control Center agent.

Option	Description
SCC agent user	User ID for the Sybase Control Center agent.
SCC agent password	Password for the Sybase Control Center agent.
Public host/port pairs	Host/port pairs in the format host1:port1,host2:port2 , and so on.
Private host/port pairs	Host/port pairs in the format host1:port1,host2:port2 , and so on.
Role	Reader or writer.
Status	Included or excluded.
Local temp dbspace path	Temporary store path.
Local temp dbspace size (MB)	Size, in megabytes, of the temporary IQ store. 0 if you select a raw device.
Local temp dbspace reserve (MB)	The amount of space, in megabytes, to reserve for future expansion in the temporary IQ store.
Raw device	Indicates a raw disk.

6. Click **OK**.
7. (Optional) Import server definitions from a CSV file.
 - a) On the Node Definitions page of the wizard, click **Import** and specify:

Option	Description
File Name	File name of the CSV file containing delimited list of server definitions.
Browse	Opens a window where you locate the CSV file.
Field Delimiter	The default field delimiter is a vertical bar " ". If your CSV file uses a different field delimiter, enter it in this field.

- b) Click **OK**.
8. (Optional) Export your existing server definitions to a CSV file for safekeeping:
 - a) On the Node Definitions page of the wizard, click **Export** and specify:

Option	Description
--------	-------------

Option	Description
Field Delimiter	The default field delimiter is a vertical bar " ". You can specify a different field delimiter.

b) Click **OK**.

9. Click **Execute**.

If Sybase Control Center continues to display the converted multiplex server as a simplex, re-authenticate the simplex resource to force SCC to update its display.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Reconfiguring a Multiplex Server

Change the name, host, port, or database file location for the selected multiplex server.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Change server name, port or database location – Requires all of:</p> <ul style="list-style-type: none"> • MULTIPLEX ADMIN authority. • BACKUP authority. <p>All other changes require DBA authority.</p>

Database Version	Multiplex Privileges
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none"> • SERVER OPERATOR system privilege. • BACKUP DATABASE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select a multiplex server from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**

The Server Properties view appears.

Note:

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.
-

4. In the left pane, click **Configuration**.
5. In the **Server Name** field, enter a new name.
6. Modify the public hosts and ports and private hosts and ports:
 - a) Double-click a public or private host name and enter a new host name.
 - b) Double-click a public or private port and enter the new port number.
 - c) If necessary, click **Add** to add a new port and enter the host name and port number.
 - d) If necessary, select a public or private host and port and click **Drop** to drop the host and port.
7. In the **Database** file path field, modify the location of the .db file.
8. Click **OK**.

See also

- *Editing the Multiplex Server Configuration File* on page 379

- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Multiplex Server Properties

View or change general, configuration, and agent information, and options and values of properties for the selected multiplex server.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	View multiplex properties – None required. Modify multiplex properties – Requires one of: <ul style="list-style-type: none">• DBA authority.• MULTIPLEX ADMIN authority.

Database Version	Multiplex Privileges
SAP Sybase IQ 16.0	<p>View multiplex properties – None required.</p> <p>Modify any property on the Configuration – Requires all of:</p> <ul style="list-style-type: none"> • SERVER OPERATOR system privilege. • BACKUP DATABASE system privilege. • MANAGE MULTIPLEX system privilege. <p>Modify any property on the Options property page – Requires SERVER OPERATOR system privilege.</p> <p>Modify any property on the Request Logging property page – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE PROFILING system privileges. • SERVER OPERATOR system privileges.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Multiplex Servers**.
3. Select the multiplex server in the right pane and either:

- Click the drop-down arrow to the right of the name and select **Properties**, or,
- From the Administration Console menu bar, select **Resource > Properties**.

The Server Properties view appears.

4. View or modify the server properties.
 - Configuration changes may take several minutes to complete.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General (Read-only)	<p>Server name – Name of the server.</p> <p>Host – Host name where the server is running.</p> <p>Port – Port where the server is running.</p> <p>Database – Database name.</p> <p>Server version – Server version number.</p> <p>Platform – Platform the server is running on.</p> <p>Platform version – Version of the operating system where the server is running.</p> <p>Type – Server type: Reader, Writer, or Coordinator.</p> <p>Change – Change the node type.</p> <hr/> <p>Note: This option is unavailable on the coordinator node.</p> <hr/> <p>Status – Server status: Include or Excluded.</p> <p>Designated Failover Node – True or False. If true, then this server is the designated failover node.</p>
Configuration	<p>Server name – Name of the server.</p> <p>Public Host/Ports – Public host names and port numbers.</p> <p>Private Host/Ports – Information about private hosts and ports to be used.</p> <p>Database file path – Location of the .db file.</p>

Area	Description
Agent (Read-only)	<p>Agent registered – Indicates if the Sybase Control Center agent is registered: true or false.</p> <p>Agent authenticated – Indicates if the Sybase Control Center agent is authenticated: true or false.</p> <p>Agent status – Status of the Sybase Control Center agent: Running, Stopped, or Unknown.</p> <p>Agent host – Name of the host machine where the Sybase Control Center agent is running.</p> <p>Agent port – Port number on the host machine where the Sybase Control Center agent is running.</p> <p>Agent user – User name for authentication of the agent. Default is <i>uafadmin</i>.</p> <p>Agent process owner – The user name that owns the agent process.</p> <p>Agent home – The home directory of the Sybase Control Center agent.</p> <p>Agent version – The version of the Sybase Control Center agent.</p> <p>SCC agent plugin version – The agent plugin version of the Sybase Control Center agent.</p> <p>IQ directory – Installation directory of the IQ server with which the Sybase Control Center agent is associated.</p> <p>IQ version – Version of the IQ server with which the Sybase Control Center agent is associated.</p>
Server Properties page (Read-only)	<p>Properties – The name, value, and description of all server properties.</p>

Area	Description
Request Logging	<p>Enable request logging – Check to enable request logging.</p> <p>All connections to this server – Check to log requests from all connections to the server.</p> <p>All connections to the following database – Specify the name of a database to log requests to all connections.</p> <p>The following connections – Specify the connections to log.</p> <p>Select type of requests to log – Check the type of requests to log:</p> <ul style="list-style-type: none"> • All • Include host variables • Triggers • Connections blocked from proceeding • SQL • Procedures • Plan <hr/> <p>Note: Some types of requests have dependencies on other types. For example, if you specify Include host variables, the information listed for SQL is also logged. For details, in the <i>SAP Sybase IQ</i> documentation, see <i>sa_server_option system procedure</i> in <i>SAP Sybase IQ Reference: Building Blocks, Tables, and Procedures</i>.</p> <hr/> <p>Log file name – Specify the pathname of the log file.</p> <p>Maximum log file size – Specify the maximum size of the log file.</p> <p>Maximum number of log files – Specify the maximum number of log files.</p> <p>Overwrite the request log file if it already exists – Check to overwrite an existing log file.</p>

Area	Description
Options page	<p>Current time – The current time.</p> <p>Refresh – Click Refresh to update the current time.</p> <p>Quitting time – Enter a time for the database server to shut down. Use the same format as the current time: YYYY-MM-DD HH:NN:SS.SS</p> <p>Disable new connections – Prevent other users from connecting to the database. This may be useful for some maintenance operations.</p> <p>Remember last statement – Instruct the database server to capture the most recently prepared SQL statement for each connection to a database on the server.</p>

Area	Description
INC page (Read-only)	<p>Note: This page is not visible for coordinator node.</p> <p>Link – Describes the INC connection shown, in the format <secondary node> => <coordinator node>.</p> <p>INC state – Current state of internode communication.</p> <p>Secondary server name – Name of secondary server.</p> <p>Heartbeat frequency – Interval until the heartbeat thread wakes and cleans up the connection pool on the secondary node.</p> <p>Last successful heartbeat – Date and time of last successful heartbeat.</p> <p>Time not responding – Elapsed time since last successful heartbeat.</p> <p>Time until timeout – Time remaining until timeout occurs due to no response.</p> <p>Liveness timeout – Time, in seconds, before a heartbeat on a secondary server declares the coordinator offline if the heartbeat fails to reconnect to the coordinator after the first disconnect. This option also determines how long the coordinator keeps a global transaction in a suspended state.</p> <p>Auto exclude timeout – Timeout for auto-excluding a secondary node on the coordinator node. 0 indicates that the nodes will not be auto-excluded. This option does not apply to the designated failover node.</p> <p>Maximum connection pool size – Maximum number of connections allowed in the connection pool on a secondary node. Values can be 1 to 1000. Default is 10.</p> <p>Current connection pool size – Current number of connections in the connection pool.</p> <p>Number of idle connections – Current number of idle connections.</p> <p>Number of connections in use – Number of connections currently in use.</p> <p>Refresh – Click Refresh to update the current display.</p>

Area	Description
MIPC page (Read-only)	<p>Node – Multiplex node name.</p> <p>Public Status – Current public status of each node. Status is set to “Not responding” if communication with that node fails.</p> <p>Private Status – Current private status of each node. Status is set to “Not configured” if there is no Private TCP/IP configuration for that server.</p>

5. Click **OK**.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Failover* on page 409
- *Multiplex Privilege Summary* on page 412
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Failover

Manual failover promotes a server to act as the coordinator in the event of coordinator node failure or maintenance shutdown.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392

- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Multiplex Privilege Summary* on page 412

Designating the Failover Node

Designate the secondary server that will become the new coordinator in a failover.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none">• MANAGE MULTIPLEX system privilege.• SERVER OPERATOR system privilege.• BACKUP DATABASE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- The multiplex coordinator is running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

The designated failover node defaults to the first multiplex server added to the multiplex. If the default is not acceptable, designate a different failover node.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers**.
3. Select a multiplex from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**
4. From the left pane of the Properties window, select **General**.
5. Click **Change** next to the **Designated Failover Node** field.

6. Select a node from the list and click **Finish**.

7. Click **OK**.

See also

- *Performing Coordinator Node Failover* on page 411
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Performing Coordinator Node Failover

Manually switch the coordinator role to the designated failover node.

Prerequisites

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The multiplex server's SCC agent is registered, authenticated, and running.
- Make sure that the former coordinator process is no longer running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Warning! Performing failover while the former coordinator process is alive may cause database corruption.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers**.
3. Select a multiplex from the right pane and either:
 - Click the arrow to the right of the name and select **Failover**, or
 - From the Administration Console menu bar, select **Resource > Failover**
4. In the Failover wizard:
 - a) Specify the new role for the current coordinator after failover.
 - b) Select a new failover node.

- c) Click **Finish**.
- d) Confirm in the popup that the coordinator is not running.

See also

- *Designating the Failover Node* on page 410
- *Registering and Authenticating a Sybase Control Center Agent* on page 279
- *Authenticating a Login Account for a Managed Resource* on page 282

Multiplex Privilege Summary

A list of the system privileges and object permissions required to complete the various multiplex server tasks

Editing the Multiplex Configuration File

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Starting or Stopping a Multiplex Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

Including a Secondary Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• All of these authorities:<ul style="list-style-type: none">• MULTIPLEX ADMIN authority, and• BACKUP authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none">• MANAGE MULTIPLEX system privilege.• SERVER OPERATOR system privilege.• BACKUP DATABASE system privilege.

Excluding a Secondary Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Synchronizing a Secondary Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires both SERVER OPERATOR and BACKUP DATABASE system privileges.

Adding a Secondary Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • All of these authorities: <ul style="list-style-type: none"> • MULTIPLEX ADMIN authority. • SPACE ADMIN authority. • BACKUP authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none"> • SERVER OPERATOR system privilege. • MANAGE MULTIPLEX system privilege. • MANAGE ANY DBSPACE system privilege. • BACKUP DATABASE system privilege.

Dropping a Secondary Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • All of these authorities: <ul style="list-style-type: none"> • MULTIPLEX ADMIN authority. • SPACE ADMIN authority. • BACKUP authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none"> • MANAGE MULTIPLEX system privilege.

Generating an Administration Script for Multiplex Nodes

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Converting a Simplex Server to Multiplex

Database Version	Simplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Reconfiguring a Multiplex Server

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Change server name, port or database location – Requires all of: <ul style="list-style-type: none"> • MULTIPLEX ADMIN authority. • BACKUP authority. <p>All other changes require DBA authority.</p>

Database Version	Multiplex Privileges
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none"> • SERVER OPERATOR system privilege. • BACKUP DATABASE system privilege.

Viewing or Modifying Multiplex Server Properties

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	View multiplex properties – None required. Modify multiplex properties – Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	View multiplex properties – None required. Modify any property on the Configuration – Requires all of: <ul style="list-style-type: none"> • SERVER OPERATOR system privilege. • BACKUP DATABASE system privilege. • MANAGE MULTIPLEX system privilege. Modify any property on the Options property page – Requires SERVER OPERATOR system privilege. Modify any property on the Request Logging property page – Requires one of: <ul style="list-style-type: none"> • MANAGE PROFILING system privileges. • SERVER OPERATOR system privileges.

Designating the Failover Node

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires all of: <ul style="list-style-type: none"> • MANAGE MULTIPLEX system privilege. • SERVER OPERATOR system privilege. • BACKUP DATABASE system privilege.

Performing Coordinator Node Failover

Database Version	Multiplex Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

See also

- *Editing the Multiplex Server Configuration File* on page 379
- *Starting a Multiplex Server* on page 386
- *Stopping a Multiplex Server* on page 387
- *Including an Excluded Secondary Server* on page 388
- *Excluding a Secondary Server* on page 390
- *Synchronizing a Secondary Server* on page 391
- *Adding a Secondary Server* on page 392
- *Dropping a Secondary Server* on page 395
- *Generating Administration Scripts for Multiplex Nodes* on page 396
- *Converting a Simplex Server to Multiplex* on page 398
- *Reconfiguring a Multiplex Server* on page 400
- *Viewing or Modifying Multiplex Server Properties* on page 402
- *Failover* on page 409

Logical Servers

Manage and monitor logical servers in the SAP Sybase IQ environment.

Monitor Logical Servers

Statistics allow you to monitor the availability and performance of logical servers.

Viewing Logical Server Overview Statistics

Display the health of the logical servers in a Sybase IQ multiplex environment.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Logical Server**.
2. In the left pane of the IQ Multiplex Level Monitor view, select **Overview**.
3. Select the tab for the required information.

Note: Click a column header to sort the data by that column.

To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
Logical Server > CPU History	Percentage of total CPU usage over a period of time for each logical server. The legend below the chart identifies the colored line associated with each logical server.
Logical Server > IQ Memory	Allocation of the IQ memory between the main cache and temporary cache for each logical server in the multiplex.
Alerts	Any alerts for the selected logical server. While the monitor is open, alerts are displayed as they are created.

See also

- *Viewing Logical Server Statistics* on page 417
- *Viewing Logical Server Monitor Settings Details* on page 419

Viewing Logical Server Statistics

Display the statistics for logical servers in the Sybase IQ multiplex.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Logical Server**.
2. In the left pane of the IQ Logical Server Level Monitor view, select **Servers**.
3. In the Logical Server Nodes area, select the server to display in the Server Details area.

Note: Click a column header to sort the data by that column.

To display the information in a chart or table in the full window, select the Maximize icon in the top right of the area.

Hover the mouse pointer over any line or bar graph to display information for that graph.

Area	Description
------	-------------

Area	Description
Logical Server Nodes	<p>Server – name of the server.</p> <p>Host – host name where the server is running.</p> <p>Port – port number where the server is running.</p> <p>State – current state of the server. Valid states include:</p> <ul style="list-style-type: none"> • Unknown • Stopped • Running <p>Role – role the server plays in the multiplex configuration. Roles include:</p> <ul style="list-style-type: none"> • Coordinator • Reader • Writer <p>Status – current status of the server in the multiplex. Valid states include:</p> <ul style="list-style-type: none"> • Included • Excluded
Server Details	<p>Server name – name of the server.</p> <p>State – current state of the server. Valid states include:</p> <ul style="list-style-type: none"> • Unknown • Stopped • Running <p>Database – name of the IQ database.</p> <p>Database path – location of the database file on the server.</p> <p>Server version – version of the IQ server.</p> <p>Platform – operating system running on the host of the server.</p>

See also

- *Viewing Logical Server Overview Statistics* on page 416
- *Viewing Logical Server Monitor Settings Details* on page 419

Viewing Logical Server Monitor Settings Details

You can control the rate at which data on monitor screens and charts is refreshed, the amount of time covered by charts, and the logical servers included in charts.

1. In the Perspective Resources window, select the resource, click the arrow, and select **Monitor Logical Server**.
2. In the left pane of the IQ Logical Server Level Monitor view, select **Settings**.

Setting	Description
Screen refresh interval (Seconds)	Enter the number of seconds between refreshes. You can also use the up and down arrows to select the appropriate number of seconds. The default is 30 seconds.
Chart Trend Period	Enter the number of minutes of data to appear in charts. The minimum number of minutes is 5, and the maximum number is 999999999. The default is 30 minutes. Since data is added to a chart only when it is open, a chart contains data starting from when you opened it. Each refresh interval adds new data to the end of the graph. A chart trend period of 30 minutes shows the statistics trend over the last 30 minutes, even if the view has been open longer than 30 minutes.
Maximum Number of Nodes to Show in Chart	Enter the maximum number of nodes to include in any monitoring charts. The default is 10 nodes.
Select Nodes	Choose the nodes to include in the monitoring charts. You cannot select more than the maximum number of nodes.

See also

- *Viewing Logical Server Overview Statistics* on page 416
- *Viewing Logical Server Statistics* on page 417

Administer Logical Servers

A logical server allows you to group a subset of physical hardware resources together as a logical entity that appears as a single multiplex server, when it is actually one or more servers within the physical multiplex.

In the *SAP Sybase IQ* documentation, see *SAP Sybase IQ Administration: Multiplex > Logical Servers* for logical server concepts and logical server policy concepts.

Creating a Logical Server

Create a logical server to group multiple physical multiplex servers into a single logical entity.

Prerequisites

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Logical Servers**.
3. Click the arrow next to **Logical Servers** and select **New**.
The Create Logical Server wizard appears.
4. On the Logical Server Name page, specify:

Option	Description
Select the resource for which the logical server will be created.	List of available resources.
What do you want to name the new logical server?	Unique name for the logical server.
What would you like the comment to be for this logical server?	Optional comment about this logical server.

5. Click **Next**.
6. On the Logical Server Node Membership page, select the multiplex nodes you want to add to the logical server. You can select the coordinator node, or secondary nodes.

Note: Select the FOR LOGICAL COORDINATOR node to add the current coordinator as a member. This ensures the coordinator is always available to the logical server as its member, regardless of which multiplex node plays the coordinator role. In the *SAP Sybase*

IQ documentation, see [SAP Sybase IQ Administration: Multiplex > Manage Multiplex Servers > High Availability > Coordinator Failure](#) for information on failover.

7. Click **Finish**.

See also

- *Deleting a Logical Server* on page 421
- *Configuring Logical Server Node Membership* on page 422
- *Altering a Logical Server Assignment* on page 423
- *Generating DDL Commands for a Logical Server* on page 425
- *Viewing or Modifying Logical Server Properties* on page 426
- *Logical Server Privilege Summary* on page 427
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Logical Server

Delete a logical server from the database. Deleting a logical server does not delete its component multiplex nodes from the database.

Prerequisites

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Logical Servers**.
3. Select one or more logical servers from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**

Tip: Use **Shift-click** or **Control-click** to select multiple logical servers.

4. Click **Yes** to confirm deletion.

See also

- *Creating a Logical Server* on page 420
- *Configuring Logical Server Node Membership* on page 422
- *Altering a Logical Server Assignment* on page 423
- *Generating DDL Commands for a Logical Server* on page 425
- *Viewing or Modifying Logical Server Properties* on page 426
- *Logical Server Privilege Summary* on page 427
- *Authenticating a Login Account for a Managed Resource* on page 282

Configuring Logical Server Node Membership

Add or remove multiplex nodes to or from the logical server.

Prerequisites

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.
- Be familiar with the restrictions and rules regarding which coordinator, reader, and writer nodes you can add to a logical server. In the SAP Sybase IQ documentation, see *SAP Sybase IQ Administration: Multiplex > Manage Resources Through Logical Servers*.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Logical Servers**.
3. Select the logical server from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**

The Logical Server Properties view appears.

Note:

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

4. In the left pane, click **Multiplex Nodes**.
5. Select or clear multiplex nodes to modify the logical server configuration.

Note: Select the FOR LOGICAL COORDINATOR node to add the current coordinator as a member. This ensures the coordinator is always available to the logical server as its member, regardless of which multiplex node plays the coordinator role. In the SAP Sybase IQ documentation, see *SAP Sybase IQ Administration: Multiplex > Manage Multiplex Servers > High Availability > Coordinator Failure* for information on failover.

6. Click **OK**.

See also

- *Creating a Logical Server* on page 420
- *Deleting a Logical Server* on page 421
- *Altering a Logical Server Assignment* on page 423
- *Generating DDL Commands for a Logical Server* on page 425
- *Viewing or Modifying Logical Server Properties* on page 426
- *Logical Server Privilege Summary* on page 427
- *Authenticating a Login Account for a Managed Resource* on page 282

Altering a Logical Server Assignment

Add one or more user-defined logical servers to a login policy. A check prevents membership overlap among the logical servers assigned to the login policy.

Prerequisites

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Login Policies**.
3. Select the login policy from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**

The Login Policy Properties view appears.

Note:

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.
-

4. (Optional) On the General Properties page, enter a comment for this login policy.
5. In the left pane, click **Logical Server Assignment** and specify:

Option	Description
Which logical servers do you want to add to this login policy?	<p>CUSTOM – Allows access to OPEN and user-defined logical servers.</p> <p>DEFAULT – Inherits the logical server assignment of the root login policy.</p> <p>NONE – Disallows access to all logical servers.</p> <p>SERVER – Allows access to any multiplex node. MPX authority is required to connect.</p>
Modify logical server assignment for a login policy	Select the logical servers to add to the login policy.

6. Click **OK**.

See also

- *Creating a Logical Server* on page 420
- *Deleting a Logical Server* on page 421
- *Configuring Logical Server Node Membership* on page 422
- *Generating DDL Commands for a Logical Server* on page 425
- *Viewing or Modifying Logical Server Properties* on page 426
- *Logical Server Privilege Summary* on page 427

- *Authenticating a Login Account for a Managed Resource* on page 282

Generating DDL Commands for a Logical Server

Display the SQL data description language for creating a new logical server. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Logical Servers**.
3. Select the logical server from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**

Tip: Use **Shift-click** or **Control-click** to select multiple logical servers.

The DDL view opens, showing the SQL code used to create the selected logical servers.

See also

- *Creating a Logical Server* on page 420
- *Deleting a Logical Server* on page 421
- *Configuring Logical Server Node Membership* on page 422
- *Altering a Logical Server Assignment* on page 423
- *Viewing or Modifying Logical Server Properties* on page 426
- *Logical Server Privilege Summary* on page 427
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Logical Server Properties

View or change the properties of the multiplex nodes associated with a logical server.

Prerequisites

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	View logical server properties – None required. Modify logical server properties – Requires one of: <ul style="list-style-type: none">• DBA authority.• MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	View any logical server property page – None required. Modify any logical server property – Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Logical Servers**.
3. Select the logical server from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**

The Logical Server Properties view appears.

4. View or modify the properties.
 - Configuration changes may take several minutes to complete.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) The name of the logical server.</p> <p>LS Policy – (Read-only for the Coordinator and Open nodes) Logical server policies to select.</p> <p>Comment – A text field for adding an optional comment about the logical server.</p>
Multiplex Nodes	<p>Note: The properties on this page are read-only for the Coordinator and Open nodes.</p> <p>Shows the available multiplex nodes. Nodes included in the current logical server are selected. Change selections to change member nodes.</p>

5. Click **OK**.

See also

- *Creating a Logical Server* on page 420
- *Deleting a Logical Server* on page 421
- *Configuring Logical Server Node Membership* on page 422
- *Altering a Logical Server Assignment* on page 423
- *Generating DDL Commands for a Logical Server* on page 425
- *Logical Server Privilege Summary* on page 427
- *Authenticating a Login Account for a Managed Resource* on page 282

Logical Server Privilege Summary

A list of the system privileges and object permissions required to complete the various logical server tasks

Creating a Logical Server

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Deleting a Logical Server

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Configuring Logical Server Node Membership

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Altering a Logical Server Assignment

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Generating DDL Commands for a Logical Server

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Logical Server Properties

Database Version	Logical Server Privileges
SAP Sybase IQ 15.3 and 15.4	View logical server properties – None required. Modify logical server properties – Requires one of: <ul style="list-style-type: none"> • DBA authority. • MULTIPLEX ADMIN authority.
SAP Sybase IQ 16.0	View any logical server property page – None required. Modify any logical server property – Requires MANAGE MULTIPLEX system privilege.

See also

- *Creating a Logical Server* on page 420
- *Deleting a Logical Server* on page 421
- *Configuring Logical Server Node Membership* on page 422
- *Altering a Logical Server Assignment* on page 423
- *Generating DDL Commands for a Logical Server* on page 425
- *Viewing or Modifying Logical Server Properties* on page 426

Administer Logical Server Policies

A logical server policy is associated with each logical server. Configure logical server policy options to control behavior of all associated logical servers.

Creating a Logical Server Policy

Control behavior of all logical servers associated with a new logical server policy.

Prerequisites

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Logical Server Policies**.
3. Click the arrow next to **Logical Server Policies** and select **New**.
4. In the Logical Server Policy wizard, specify:

Option	Description
Select the resource for which the logical server policy will be created.	List of multiplex servers.
What do you want to name the new logical server policy?	Unique name for the logical server policy.

Option	Description
<p>What options would you like to set for this logical server policy?</p>	<p>(Optional.)</p> <p>Login Redirection – When ON, enables login redirection for logical servers governed by specified login policy. When OFF (the default), disables login redirection.</p> <p>Temp Data in Shared Temp – When ON (the default), all temporary table data and eligible scratch data writes to the shared temporary store if it is not empty. (If the shared temporary store contains no read-write file, data instead writes to IQ_SYSTEM_TEMP.) When OFF, all temporary table data and scratch data writes to the local temporary store.</p> <p>DQP Enabled – Specify DQP disabled, Enable DQP with shared temp (the default), or Enable DQP over the network.</p> <p>You can reset this option dynamically. Distributed query processing (DQP) over the network keeps data in memory in the temporary cache instead of in the IQ_SHARED_TEMP dbspace. The option that provides the best performance may vary by query, and depends on the performance of the network relative to the I/O system.</p> <p>Redirection Waiters Threshold – Specify how many connections can queue before SAP Sybase IQ redirects a connection to this logical server. Use an integer value (default is 5).</p>
<p>What would you like the comment to be for this logical server?</p>	<p>Enter an optional comment to simplify logical server policy administration</p>

5. Click **Finish**.

See also

- *Deleting a Logical Server Policy* on page 432
- *Generating DDL Commands for a Logical Server Policy* on page 433
- *Viewing or Modifying Logical Server Policy Properties* on page 434
- *Logical Server Policy Privilege Summary* on page 436
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Logical Server Policy

Delete a logical server policy from the database.

Prerequisites

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires <code>MANAGE MULTIPLEX</code> system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- No logical servers currently use the policy
- The target is not the root logical server policy
- You are licensed for the Multiplex Grid option (`IQ_MPXNODE`), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Logical Server Policies**.
3. Select one or more logical server policy from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**

Tip: Use **Shift-click** or **Control-click** to select multiple logical server policies.

4. Click **Yes** to confirm deletion.

See also

- *Creating a Logical Server Policy* on page 429
- *Generating DDL Commands for a Logical Server Policy* on page 433
- *Viewing or Modifying Logical Server Policy Properties* on page 434
- *Logical Server Policy Privilege Summary* on page 436
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating DDL Commands for a Logical Server Policy

Display the SQL data description language for creating one or more logical server policies. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Logical Server Policies**.
3. Select one or more logical server policy from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**

Tip: Use **Shift-click** or **Control-click** to select multiple logical server policies.

The DDL view opens, showing the SQL code used to create the selected logical server policies.

See also

- *Creating a Logical Server Policy* on page 429
- *Deleting a Logical Server Policy* on page 432
- *Viewing or Modifying Logical Server Policy Properties* on page 434
- *Logical Server Policy Privilege Summary* on page 436
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Logical Server Policy Properties

View or change behavior such as distributed query processing for servers associated with a logical server policy.

Prerequisites

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	View any logical server policy property page – None required. Modify any logical server policy property – Requires MANAGE MULTIPLEX system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Multiplex Grid option (IQ_MPXNODE), if running secondary servers.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Multiplex Management > Logical Server Policies**.
3. Select the logical server policy from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**

The Logical Server Policy Properties view appears.

4. View or modify the properties.
 - Configuration changes may take several minutes to complete.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) Name of the logical server policy.</p> <p>Options:</p> <ul style="list-style-type: none"> • Allow Coordinator As Member – (Root policy only) – When ON (the default), the coordinator can be a member of any user-defined logical server. OFF prevents the coordinator from being a member of any user-defined logical servers. • (16.0 only) Login Redirection – When ON, enables login redirection for logical servers governed by specified login policy. When OFF (the default), disables login redirection. • (16.0 only) Temp Data in Shared Temp – When ON (the default), all temporary table data and eligible scratch data writes to the shared temporary store if it is not empty. (If the shared temporary store contains no read-write file, data instead writes to IQ_SYSTEM_TEMP.) When OFF, all temporary table data and scratch data writes to the local temporary store. <p>If you change the value of Temp Data in Shared Temp, you must restart all servers that belong to this logical server. After the restart, each server that is part of the logical server begins putting temporary table data in the appropriate store.</p> <ul style="list-style-type: none"> • (16.0 only) DQP Enabled – Specify DQP disabled, Enable DQP with shared temp (the default), or Enable DQP over the network. <p>You can reset this option dynamically. Distributed query processing (DQP) over the network keeps data in memory in the temporary cache instead of in the IQ_SHARED_TEMP dbspace. The option that provides the best performance may vary by query, and depends on the performance of the network relative to the I/O system.</p> <ul style="list-style-type: none"> • (16.0 only) Redirection Waiters Threshold – Defaults to 5. Positive integer value that specifies how many connections can queue before SAP Sybase IQ redirects a connection to this logical server to another server. <p>Comment – Enter an optional comment to simplify logical server policy administration.</p>

5. Click **OK**.

See also

- *Creating a Logical Server Policy* on page 429
- *Deleting a Logical Server Policy* on page 432
- *Generating DDL Commands for a Logical Server Policy* on page 433
- *Logical Server Policy Privilege Summary* on page 436
- *Authenticating a Login Account for a Managed Resource* on page 282

Logical Server Policy Privilege Summary

A list of the system privileges and object permissions required to complete the various logical server policy tasks

Creating a Logical Server Policy

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Deleting a Logical Server Policy

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE MULTIPLEX system privilege.

Generating DDL Commands for a Logical Server Policy

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Logical Server Policy Properties

Database Version	Logical Server Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	View any logical server policy property page – None required. Modify any logical server policy property – Requires MANAGE MULTIPLEX system privilege.

See also

- *Creating a Logical Server Policy* on page 429
- *Deleting a Logical Server Policy* on page 432
- *Generating DDL Commands for a Logical Server Policy* on page 433
- *Viewing or Modifying Logical Server Policy Properties* on page 434

Remote Servers

A remote server allows you to set up access to remote database objects, using external logins, proxy tables and remote procedures.

For some systems, including Sybase IQ and SQL Anywhere, each data source describes a database; therefore, you must define a separate remote server definition for each database.

See also

- *Creating a Remote Procedure* on page 1254
- *Creating a Proxy Table* on page 479
- *Creating an External Login* on page 446

Creating a Remote Server

Before you can map remote objects to a local proxy table, you must define the remote server where the remote object is located.

Prerequisites

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

For some systems, including SAP Sybase IQ and SQL Anywhere, each data source describes a database; therefore, you must define a separate remote server definition for each database.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Networks > Remote Servers**.
3. Click the arrow next to **Remote Servers** and select **New**.
The Create Remote Server wizard appears.
4. On the Name and Type page, specify:

Option	Description
Resource	The local server that will contain the remote server definition. (The resource from which you want to access the database housed on the remote server).
Remote Server Name	The local name used for connecting to the server where the remote database is located.
Type	The type of server where the remote database is located.

5. Click **Next**.
6. On the Connection Details page, specify:

Option	Description
Connection Type	Select Open Database Connectivity (ODBC) or Java Database Connectivity (JDBC).
Connection Information	Enter either the data source name (OBDC) or <code>host:port/db</code> connection string (JDBC).

Note: The Remote Server Type you specified on the Name and Type page may limit the connection type. The only server types allowing a JDBC connection are SAP Sybase IQ, SQL Anywhere and Adaptive Server Enterprise servers. However, for IQ server versions 16.0 and above, JDBC is not supported.

7. Click **Next**.
8. On the Read-Only Option page of the wizard, select the check-box if you want to define the remote server as a read-only data source.
9. Click **Next**.
10. On the External Login page of the wizard, select the check-box if you want to enter an alternate login name and password for your user ID (recommended).

Option	Description
Login name	The alternate user ID to be used on the remote server.
Password	The password for validating the alternate user ID on the remote server. The password is optional, but recommended.
Confirm password	If you enter a password, re-type it as verification.

Note: You can create external logins for other locally defined users with the Create External Login wizard.

11. Click Finish.**See also**

- *Testing a Remote Server Connection* on page 439
- *Deleting a Remote Server* on page 440
- *Generating Remote Server DDL Commands* on page 441
- *Viewing or Modifying Remote Server Properties* on page 442
- *Remote Server Privilege Summary* on page 444
- *Creating an External Login* on page 446
- *Creating a Remote Procedure* on page 1254
- *Creating a Proxy Table* on page 479
- *Authenticating a Login Account for a Managed Resource* on page 282

Testing a Remote Server Connection

Test the physical connection to one or more remote servers.

Prerequisites

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Networks > Remote Servers**.
3. Select one or more remote servers from the right pane and either:
 - Click the arrow to the right of the name and select **Test Connection**, or
 - From the Administration Console menu bar, select **Resource > Test Connection**

Tip: Use **Shift-click** or **Control-click** to select multiple remote servers.

The physical connection to each selected remote server is tested, and connection status displays.

See also

- *Creating a Remote Server* on page 437

- *Deleting a Remote Server* on page 440
- *Generating Remote Server DDL Commands* on page 441
- *Viewing or Modifying Remote Server Properties* on page 442
- *Remote Server Privilege Summary* on page 444
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Remote Server

Remove one or more existing Remote Server definitions, along with all associated proxy tables, remote procedures and external login definitions.

Prerequisites

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Networks > Remote Servers**.
3. Select one or more remote servers from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**

Tip: Use **Shift-click** or **Control-click** to select multiple remote servers.

4. Click **Yes** to confirm deletion.

Note: The remote server definition is deleted, along with all associated proxy tables, remote procedures and external login definitions.

See also

- *Creating a Remote Server* on page 437
- *Testing a Remote Server Connection* on page 439
- *Generating Remote Server DDL Commands* on page 441
- *Viewing or Modifying Remote Server Properties* on page 442
- *Remote Server Privilege Summary* on page 444

- *Creating an External Login* on page 446
- *Creating a Proxy Table* on page 479
- *Creating a Remote Procedure* on page 1254
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Remote Server DDL Commands

Generate data description language for one or more remote servers. The DDL can be a useful resource and training tool.

Prerequisites

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Networks > Remote Server**.
3. Select the remote server from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**

The DDL view opens, showing the SQL code used to create the selected remote server.

See also

- *Creating a Remote Server* on page 437
- *Testing a Remote Server Connection* on page 439
- *Deleting a Remote Server* on page 440
- *Viewing or Modifying Remote Server Properties* on page 442
- *Remote Server Privilege Summary* on page 444
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Remote Server Properties

Display or change the properties of the selected remote server definition.

Prerequisites

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	View remote server properties – None required. Modify remote server properties – Requires DBA authority.
SAP Sybase IQ 16.0	View any remote server property page – None required. Modify any remote server property – Requires SERVER OPERATOR system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Networks > Remote Servers**.
3. Select the remote server from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**

The Remote Server Properties view appears.

4. View the properties, including the defined proxy tables, remote procedures and external logins associated with the remote server, by navigating to the corresponding page on the Remote Server Properties view. On any page, by selecting a proxy table, remote procedure, or external login and clicking the corresponding button, you can **Edit**, **Delete**, **Generate DDL** or **View Data in SQL**.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) The local name used for connecting to the server where the remote database is located, as specified when the remote server was created.</p> <p>Read-Only – (Read-only) Indicates whether the remote server is a read-only data source, as specified when the remote server was created.</p> <p>Server Type – The type of server where the remote database is located.</p> <p>Connection Type – The Remote Server Type you specify may limit the connection type. The only server types allowing a JDBC connection are Sybase IQ, SQL Anywhere and Sybase ASE servers. However, for IQ server versions 16.0 and above, JDBC is not supported.</p> <p>Connection Information – Use the Test Connection button to validate the connection information.</p>
Proxy tables	<p>Name – The local name used for the object on the remote database</p> <p>Owner – The specified user ID owning the object.</p> <p>Location – The server on which the remote database resides.</p> <p>Comment – Additional description or information.</p>
Remote procedures	<p>Name – The local name used for the procedure on the remote database</p> <p>Owner – The specified user ID owning the procedure.</p> <p>Comment – Additional description or information</p>
External logins	<p>User – The defined local user for whom the alternate login name and password (external login) was created</p> <p>Login Name – The user ID used on the remote server by the User.</p>

5. Click **OK**.

See also

- *Creating a Remote Server* on page 437
- *Testing a Remote Server Connection* on page 439
- *Deleting a Remote Server* on page 440
- *Generating Remote Server DDL Commands* on page 441
- *Remote Server Privilege Summary* on page 444

- *Creating a Remote Procedure* on page 1254
- *Creating an External Login* on page 446
- *Creating a Proxy Table* on page 479
- *Authenticating a Login Account for a Managed Resource* on page 282

Remote Server Privilege Summary

A list of the system privileges and object permissions required to complete the various remote server tasks

Creating a Remote Server

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

Testing a Remote Server Connection

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Deleting a Remote Server

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires SERVER OPERATOR system privilege.

Generating Remote Server DDL Commands

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Remote Server Properties

Database Version	Remote Server Privileges
SAP Sybase IQ 15.3 and 15.4	View remote server properties – None required. Modify remote server properties – Requires DBA authority.
SAP Sybase IQ 16.0	View any remote server property page – None required. Modify any remote server property – Requires SERVER OPERATOR system privilege.

See also

- *Creating a Remote Server* on page 437
- *Testing a Remote Server Connection* on page 439
- *Deleting a Remote Server* on page 440
- *Generating Remote Server DDL Commands* on page 441
- *Viewing or Modifying Remote Server Properties* on page 442

External Logins

External logins are alternate login names and passwords to be used when communicating with a remote server (in order to set up access to remote database objects).

By default, IQ uses the names and passwords of its clients whenever it connects to a remote server or directory access server on behalf of those clients. However, you can override this default by creating external logins.

Note: You must define a remote server before you can create an external login.

When you create a remote server definition, you have the option of creating an external login for your user ID. Using the Create External Login wizard, you can create external logins for other user IDs

See also

- *Creating a Proxy Table* on page 479
- *Creating a Remote Procedure* on page 1254
- *Creating a Remote Server* on page 437

Creating an External Login

Define an alternate login name and password by specifying the remote server to create an external login for, and the local user the external login applies to.

Prerequisites

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

- The SAP Sybase IQ resource is authenticated and running. (The resource on which you are creating the external login).

Note: You must define a remote server before you can create an external login.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Networks > External Logins**.
3. Click the arrow next to **External Logins** and select **New**.
The Create External Login Wizard appears.
4. On the Server and User page, specify:

Option	Description
Resource	The resource (server) that the external login will be created on.
Remote Server	The defined remote server which the external login will be used to connect to.
User	The defined local user for whom the alternate login name and password (external login) will be created.

5. Click **Next**.
6. On the External Login page, specify:

Option	Description
Login name	The user ID to be used on the remote server by the previously selected locally defined user.
Password	The password for validating the user ID on the remote server. If the user has no password on the remote server , leave it blank.
Confirm password	If you enter a password, re-type it as verification.

7. Click **Finish**.

See also

- *Deleting an External Login* on page 447
- *Generating External Login DDL Commands* on page 448
- *Viewing External Login Properties* on page 449
- *External Login Privilege Summary* on page 450
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting an External Login

Delete one or more external login definitions.

Prerequisites

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Networks > External Logins**.
3. Select one or more external logins from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**

Tip: Use **Shift-click** or **Control-click** to select multiple external logins.

4. Click **Yes** to confirm deletion.

See also

- *Creating an External Login* on page 446
- *Generating External Login DDL Commands* on page 448
- *Viewing External Login Properties* on page 449
- *External Login Privilege Summary* on page 450
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating External Login DDL Commands

Generate data description language for one or more external login. The DDL can be a useful resource and training tool.

Prerequisites

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Networks > External Logins**.
3. Select the external login from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**

Tip: Use **Shift-click** or **Control-click** to select multiple external logins.

The DDL view opens, showing the SQL code used to create the selected external login(s).

See also

- *Creating an External Login* on page 446
- *Deleting an External Login* on page 447
- *Viewing External Login Properties* on page 449
- *External Login Privilege Summary* on page 450
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing External Login Properties

Display the properties of an existing external login definition.

Prerequisites

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Networks > External Logins**.
3. Select an external login from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**

The External Login Properties view appears (read-only).

4. View the properties of the external login.

Area	Description
Remote Server	The local name used for connecting to the server where the remote database is located.
Local User Name	The defined local user for whom the alternate login name and password (external login) was created
Remote Login Name	The user ID used on the remote server by the local user.

5. Click **OK**.

See also

- *Creating an External Login* on page 446
- *Deleting an External Login* on page 447
- *Generating External Login DDL Commands* on page 448
- *External Login Privilege Summary* on page 450

- *Authenticating a Login Account for a Managed Resource* on page 282

External Login Privilege Summary

A list of the system privileges and object permissions required to complete the various external login tasks

Creating an External Login

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Deleting an External Login

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Generating External Login DDL Commands

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing External Login Properties

Database Version	External Login Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

See also

- *Creating an External Login* on page 446

- *Deleting an External Login* on page 447
- *Generating External Login DDL Commands* on page 448
- *Viewing External Login Properties* on page 449

Databases

Create a database and view database options and properties.

Appropriate system privileges are required for all database management tasks.

Note: An SAP Sybase IQ server resource cannot have multiple databases. Attempting to manage, monitor, or administer an SAP Sybase IQ server resource connected to multiple databases may cause unexpected results.

Creating a Database

Use the Create Databases wizard to create an SAP Sybase IQ database on the same host as the SCC agent.

Prerequisites

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	Required DBA authority. The account under which the server is running must have write permissions on the directories where files are created.
SAP Sybase IQ 16.0	The account under which the server is running must have write permissions on the directories where files are created. No other system privilege is required.

- The SAP Sybase IQ resource is authenticated and running.

Task

Successful database creation results in a new, running, and registered SAP Sybase IQ server visible in the resource perspective.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Databases**.
3. Click the arrow next to **Databases** and select **New**.
The Create Databases wizard appears.
4. On the Database Definitions page, click **Add**, and specify:

Option	Description
Host	The name of the host system where the new database is created.
SCC agent port	The port number that the Sybase Control Center agent on the given host is listening on. Default is 9999 .
SCC agent user	User ID for the Sybase Control Center agent. Default is uafadmin .
SCC agent password	Password for the Sybase Control Center agent user. Default is no password.
Utility server user	User ID for the utility database. Default is DBA .
Utility server password	Password for the utility database. Default is sql .
IQ Server Name	Name of the IQ server to be created.
IQ Server Port	Port number for the new IQ server.
IQ user	User ID for the new IQ server.
IQ password	User password for the IQ user.
Database path	Path to the database file. For example, /<hostname>/sample/sample/mytestdb.db .
IQ page size	Page size of the database, in kilobytes. If you do not make a selection, the application chooses a page size. Default is 128.
Catalog page size	Database page size for the catalog store, in kilobytes. If you do not make a selection, the application automatically chooses a page size. Default is 4.
IQ main dbspace path	Path to the IQ main store dbspace physical file on disk. For example, /<hostname>/sample/sample/mytestdb.iq .
IQ main dbspace size (MB)	(Disabled if Raw Device is selected.) The amount of space, in megabytes, for the IQ main store dbspace. Specify at least 100 . Default is 1000
IQ main dbspace reserve (MB)	(Disabled if Raw Device is selected.) The amount of space, in megabytes, to reserve for future expansion in the IQ main store. Default is 300.
Raw device (IQ main dbspace)	Indicates a raw disk. Default is selected.

Option	Description
Local temporary dbspace path	Path to the temporary IQ store physical file on disk. For example: <code>/<hostname>/sample/sample/mytestdb.iqtmp</code> .
Local temporary dbspace size (MB)	(Disabled if Raw Device is selected.) Size, in megabytes, for the temporary IQ store. Default is 1000.
Local temporary dbspace reserve (MB)	The amount of space, in megabytes, to reserve for future expansion in the temporary IQ store. Default is 300.
Raw device (Local temp dbspace)	Indicates a raw disk. Default is selected.
Transaction log	File name of the IQ transaction log that records changes to the database. If you leave this field blank, the application automatically assigns a log name: <code><database_name>.log</code> .
Transaction mirror log	File name of the copy of the default transaction log, stored on another device, for additional security. The default mirror log name is <code><database_name>.mlg</code>
CHAR collation	Click Select to open the Select CHAR Collation dialog box. (Select is disabled until all required fields are filled.) In the dialog box, select the CHAR collation sequence used by the database to perform alphanumeric sorting. The default is ISO_BINENG . If you select UCA (Unicode Collation Algorithm), you are prompted to specify how the database should treat accents.
NCHAR collation	Click Select to open the Select NCHAR Collation dialog box. (Select is disabled until all required fields are filled.) In the dialog box, select the NCHAR collation sequence used by the database to perform alphanumeric sorting on NCHAR data. The default is UCA . If you select UCA (Unicode Collation Algorithm) you are prompted to specify how the database should treat accents.

5. (Optional) Click **Settings** and specify:

Option	Description
Encryption	Specify whether to create the database with no encryption, simple encryption or strong encryption. Default is Simple encryption.
Algorithm	(Available for Strong encryption only) Specify an encryption algorithm. Default is AES-128
Encryption Key	If you select strong encryption, enter and confirm an encryption key.
Case Insensitivity	Specify whether the database should have case insensitivity when comparing strings. Default is enabled.
Create Views	Specify whether the database should create SYSCOLUMN and SYSINDEXES views. Default is enabled.
Ignore Trailing Blanks	Specify whether the database should ignore blank spaces at the end of strings. Default is selected. Default is not disabled.
Include Checksum	Specify whether the database should include checksum with each database page. Default is disabled.
SQL Anywhere Defaults	Select to have the options default to SQL Anywhere settings.
Emulate ASE	Select to have the options default to Adaptive Server Enterprise settings.

6. Click **OK** to close the Options view.
7. Click **OK** to close the Add Database Definition view.

The Create Database wizard remains displayed and the new database appears in the Data Definitions pane. If your database definition values are valid, a check mark appears in the Validation column. If any input for the database definition is invalid, an X appears. Hover the mouse over the X to see error information. To correct error, select the applicable database definition and click **Edit**

8. (Optional) Export your existing database definitions to a CSV file for safekeeping or future import. On the Database Definitions page of the Create Database wizard, click **Export**, specify the field delimiter and click **OK**.
9. Once the database definition is deemed valid (check mark appears), click the **Next** button.
10. On the Execution page, click **Execute** to start the database creation process.
11. Click **Close** to exit the Create Database wizard.

See also

- *Creating a Database Using a CSV File* on page 455
- *Setting Database Options* on page 456

- *Viewing or Modifying Database Properties* on page 457
- *Database Privilege Summary* on page 463
- *My Database Definition is Invalid* on page 1341
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Database Using a CSV File

Use a CSV file in the Create Databases wizard to create an SAP Sybase IQ database on the same host as the SCC agent.

Prerequisites

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	Required DBA authority. The account under which the server is running must have write permissions on the directories where files are created.
SAP Sybase IQ 16.0	The account under which the server is running must have write permissions on the directories where files are created. No other system privilege is required.

- The SAP Sybase IQ resource is authenticated and running.
- A CSV file containing the required database values.

Task

Successful database creation results in a new, running, and registered SAP Sybase IQ server visible in the resource perspective.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Databases**.
3. Click the arrow next to **Databases** and select **New**.
The Create Databases wizard appears.
4. On the Database Definitions page, click **Import**, specify the CSV file and path and the file field delimiter and click **OK**.
The new database appears in the Data Definitions pane. If your database definition values are valid, a check mark appears in the Validation column. If any input for the database definition is invalid, an X appears. Hover the mouse over the X to see error information. To correct error, select the applicable database definition and click **Edit**. See *Creating a Database* for details individual properties.
5. Once the database definition is deemed valid (check mark appears), click the **Next** button.
6. On the Execution page, click **Execute** to start the database creation process.
7. Click **Close** to exit the Create Database wizard.

See also

- *Creating a Database* on page 451
- *Setting Database Options* on page 456
- *Viewing or Modifying Database Properties* on page 457
- *Database Privilege Summary* on page 463
- *Authenticating a Login Account for a Managed Resource* on page 282

Setting Database Options

Adjust the configurable settings of a database to change the way the database behaves or performs.

Prerequisites

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	View database options only – None required. Modify database options – Requires DBA authority.
SAP Sybase IQ 16.0	View database options only – None required. Modify database options – Depending on the option being modified, requires one of: <ul style="list-style-type: none">• SET ANY PUBLIC OPTION system privilege.• SET ANY SECURITY OPTION system privilege.• SET ANY SYSTEM OPTION system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

Some database options can only be set at one level, be it database (PUBLIC) or user, while others can be set at either level.

For database options that can be set at either level, when set at the user level, the setting overrides the current value for that user only. When set it at the database level, the value becomes the new default, and is applied to any existing users who have not had the option overridden at the user level.

For information on the level at each option can be set and the system privilege required, in the SAP Sybase IQ 16.x documentation, see the alphabetical list of Database options in *SAP Sybase IQ Reference: Building Blocks, Tables, and Procedures*.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Schema Objects > Databases**.
3. Select a database from the right pane and either:
 - Click the drop-down arrow to the right of the name and select **Options**, or,
 - From the Administration Console menu bar, select **Resource > Options**.

The Options for Database "X" view appears.

4. Click in the Setting column to modify an option value.
5. Click **Apply** to save your changes and keep editing, or click **OK** to save and close the Database Options view.

See also

- *Creating a Database* on page 451
- *Creating a Database Using a CSV File* on page 455
- *Viewing or Modifying Database Properties* on page 457
- *Database Privilege Summary* on page 463
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Database Properties

View editable and non-editable properties for the database.

Prerequisites

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View database license management property page – Requires EXECUTE permission on the sp_iqlmconfig system procedure to display content of page.</p> <p>View any other database property page – None required.</p> <p>Modify the following properties on the Settings page requires:</p> <ul style="list-style-type: none"> • Include SQL statement information option – Requires EXECUTE permission on the sa_server_option system procedure to modify this setting. • Collect Information about deadlocks option – Requires DBA authority. • Clear Deadlock Information Now option – Requires DBA authority. <p>Modify any other database property – Requires DBA authority.</p>

Database Version	Database Privileges
SAP Sybase IQ 16.0	<p>View database license management property page –</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sp_iqlm-config system procedure to display content of page. • If the system procedure security model* of the selected database is set to Invoker, you require the SERVER OPERATOR system privilege to display content of page. <p>View any other database property page – None required.</p> <p>Modify the following properties on the Settings page requires:</p> <ul style="list-style-type: none"> • Refresh button – Requires SERVER OPERATOR or ALTER DATABASE system privilege. • Collect Information about deadlocks option – Requires SET ANY SYSTEM OPTION system privilege. • Include SQL statement information option – <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_server_option system procedure to modify this setting. • If the system procedure security model* of the selected database is set to Invoker, you require the SERVER OPERATOR system privilege to display content of page. • Clear Deadlock Information Now option – Requires SERVER OPERATOR system privilege. <p>Modify properties on the license management page –</p> <ul style="list-style-type: none"> • Requires SERVER OPERATOR system privilege. <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane of the Administration Console, select **IQ Servers > Schema Objects > Databases**.
3. Select the database from the right pane and either:

- Click the drop-down arrow to the right of the name and select **Properties**, or,
- From the Administration Console menu bar, select **Resource > Properties**.

The Database Properties view appears.

4. View or modify the properties.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Database – Name of the database.</p> <p>ID – A unique number assigned by the server to each database that is started on it. The ID number lets you distinguish between databases running on the same server.</p> <p>Capability ID – The capability bits enabled for the database. You can view a list of the capabilities that are enabled for the database on the Extended Information tab of the Database property sheet.</p> <p>Java location – Path to the JRE executable file.</p> <p>Java main user ID – The main Java user ID.</p> <p>Page size – Page size of the database, in bytes.</p> <p>Database file – Root database file for the database.</p> <p>Log file – Name and location of the transaction log file for the database.</p> <p>Mirror log file – Name and location of the mirror log file for the database.</p> <p>Temporary file – Location of the temporary database file.</p> <p>Current user – User ID of the user connected to the database.</p> <p>Connection ID – Connection ID for the database connection from Sybase Control Center.</p> <p>Connection name – Connection name for the user connected to this database. Naming your connections allows multiple connections to the same database, or multiple connections to the same or different database server, to be easily identified.</p> <p>Communication link – Type of communications link used by the user's connection. If the connection is between a client and network server, the link type represents the network protocol being used.</p> <p>Total connections – Total number of current connections to the database from all users, including the Sybase Control Center connection.</p> <p>(16.0 only) System procedure security model – The security model under which privileged system procedures execute. Valid values are:</p> <ul style="list-style-type: none"> • Invoker – all privileged system procedures run with the privileges of the person executing the procedure (invoker).

Area	Description
(Read-only)	<ul style="list-style-type: none">• Definer – All pre-16.0 privileged system procedures run with the privileges of the owner of the procedure (definer). All privileged system procedures introduced in 16.0 (or later) run with the privileges of the invoker.

Area	Description
Settings	<p>Encryption type – Type of database encryption: Simple or AES. If encryption is not supported in the database, the value is None.</p> <p>Encryption scope – Scope of the encryption.</p> <p>Ignore trailing blanks – Database ignores trailing blanks in comparisons.</p> <p>CHAR collation sequence – Set of separators for the collation sequence of CHAR values.</p> <p>CHAR collation character set encoding – Character set used for CHAR values.</p> <p>CHAR case sensitivity – CHAR values in the database are case-sensitive. This property applies to the data in the database, and to passwords, but not to table names, column names, and other identifiers.</p> <p>NCHAR collation sequence – Separators for the collation sequence of NCHAR values.</p> <p>NCHAR collation character set encoding – Character set used for NCHAR values.</p> <p>NCHAR case sensitivity – NCHAR values in the database are case-sensitive. This property applies to the data in the database, and to passwords, but not to table names, column names, and other identifiers.</p> <p>Checkpoint urgency(%) – Time elapsed since the last checkpoint as a percentage of the checkpoint time setting of the database.</p> <p>Recovery urgency(%) – An estimate of the amount of time required to recover the database.</p> <p>Refresh – Update the checkpoint urgency and recovery urgency values.</p> <p>Collect information about deadlocks that occur in this database – Information is collected on deadlocked connections to the database.</p> <p>Include SQL statement information for deadlocked connections – SQL statement information is included with the deadlock connection information.</p>

Area	Description
(Read-only)	Clear deadlock information now – Remove all deadlock information from the system.
Database Properties (Read-only)	A list of all database properties, including the property value and the description of the property.
License management	A list the name and value of the properties for the various licenses.

5. Click **OK**.

See also

- *Creating a Database* on page 451
- *Creating a Database Using a CSV File* on page 455
- *Setting Database Options* on page 456
- *Database Privilege Summary* on page 463
- *Authenticating a Login Account for a Managed Resource* on page 282

Database Privilege Summary

A list of the system privileges and object permissions required to complete the various database tasks.

Creating a Database

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	Required DBA authority. The account under which the server is running must have write permissions on the directories where files are created.
SAP Sybase IQ 16.0	The account under which the server is running must have write permissions on the directories where files are created. No other system privilege is required.

Creating a Database Using CSV File

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	None required.

Database Version	Database Privileges
SAP Sybase IQ 16.0	The account under which the server is running must have write permissions on the directories where files are created. No other system privilege is required.

Setting Database Options

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	View database options only – None required. Modify database options – Requires DBA authority.
SAP Sybase IQ 16.0	View database options only – None required. Modify database options – Depending on the option being modified, requires one of: <ul style="list-style-type: none"> • SET ANY PUBLIC OPTION system privilege. • SET ANY SECURITY OPTION system privilege. • SET ANY SYSTEM OPTION system privilege.

Viewing or Modifying Database Properties

Database Version	Database Privileges
SAP Sybase IQ 15.3 and 15.4	View database license management property page – Requires EXECUTE permission on the sp_iqlmconfig system procedure to display content of page. View any other database property page – None required. Modify the following properties on the Settings page requires: <ul style="list-style-type: none"> • Include SQL statement information option – Requires EXECUTE permission on the sa_server_option system procedure to modify this setting. • Collect Information about deadlocks option – Requires DBA authority. • Clear Deadlock Information Now option – Requires DBA authority. Modify any other database property – Requires DBA authority.

Database Version	Database Privileges
SAP Sybase IQ 16.0	<p>View database license management property page –</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sp_iqlm-config system procedure to display content of page. • If the system procedure security model* of the selected database is set to Invoker, you require the SERVER OPERATOR system privilege to display content of page. <p>View any other database property page – None required.</p> <p>Modify the following properties on the Settings page requires:</p> <ul style="list-style-type: none"> • Refresh button – Requires SERVER OPERATOR or ALTER DATABASE system privilege. • Collect Information about deadlocks option – Requires SET ANY SYSTEM OPTION system privilege. • Include SQL statement information option – <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_server_option system procedure to modify this setting. • If the system procedure security model* of the selected database is set to Invoker, you require the SERVER OPERATOR system privilege to display content of page. • Clear Deadlock Information Now option – Requires SERVER OPERATOR system privilege. <p>Modify properties on the license management page –</p> <ul style="list-style-type: none"> • Requires SERVER OPERATOR system privilege. <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

See also

- *Creating a Database* on page 451
- *Creating a Database Using a CSV File* on page 455
- *Setting Database Options* on page 456
- *Viewing or Modifying Database Properties* on page 457

Tables

Create, delete, and display tables (including global temporary tables and proxy tables), and manage their properties, in SAP Sybase IQ.

Tables consist of rows and columns. Each column carries a particular kind of information, such as a phone number or a name, while each row specifies a particular entry.

When a database is first created, the only tables in the database are the system tables, which hold the database schema. You can create new tables to hold your actual data.

Creating a Table

Add a base table to the database. A base table holds persistent data. (The table and its data continue to exist until you explicitly delete the data or drop the table.)

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Base table to be owned by self:</p> <ul style="list-style-type: none"> Requires RESOURCE authority with CREATE permission on the main store dbspace in which the table is created. <p>Base table to be owned by any user – Requires DBA authority.</p>
SAP Sybase IQ 16.0	<p>Base table to be owned by self –</p> <ul style="list-style-type: none"> Requires CREATE permission on the dbspace where the table is created. Also requires one of: <ul style="list-style-type: none"> CREATE TABLE system privilege. CREATE ANY OBJECT system privilege <p>Base table to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE permission on the dbspace where the table is created. Also requires one of: <ul style="list-style-type: none"> CREATE ANY TABLE system privilege. CREATE ANY OBJECT system privilege

- The SAP Sybase IQ resource is authenticated and running.
- To create tables enabled with row-level versioning (RLV), the RLV store dbspace must exist. (This is applicable in the simplex configuration of IQ 16.0 only).

- In a multiplex configuration, the coordinator node is running.

Task

Altering or creating base tables can interfere with other users of the database.

For large tables, modifying an existing table or creating a new table can be a time-consuming operation. The internal **CREATE TABLE** statement delays execution of other processes until the statement completes. Although you modify tables while other connections are active, you cannot execute them while any other connection uses the table to be altered. Modifying a table excludes other requests referencing the table being offered while the internal **ALTER TABLE** statement processes.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Click the arrow next to **Tables** and select **New**.
The Create Table wizard appears.
4. On the Welcome page, specify:

Option	Description
Select a resource for which the table will be created	From the list, select the resource for which the table will be created.
What do you want to name the table?	Enter a unique name for the new table; maximum of 128 characters.
Which user do you want to own the table?	From the list, select the user to own the table.

5. Click **Next**.
6. On the Dbspace page, specify the data store and dbspace in which the table will be created in. Only those dbspaces to which you have permissions, and only those dbspaces in read-write mode, are listed.
7. Click **Next**.
8. (For IQ store only) On the Row-level versioning (RLV) page, select **Enable RLV**, if you want the new table to use row-level versioning storage. Alternatively, select **Disable RLV** if you don't want the table to be RLV-enabled, or select **Default** if you want to use the settings from the **BASE_TABLE_IN_RLV_STORE** database option.

Note:

- Row-level versioning is supported in a simplex environment only. The row-level versioning page does not appear in a multiple environment.
- The RLV store dbspace must exist before creating RLV-enabled tables.

- Only IQ base tables are supported in the RLV store: catalog, temporary and global temporary tables are not supported.
 - LONG VARBINARY (LOB) and LONG VARCHAR data types are not supported on RLV-enabled tables.
 - TEXT and WORD indexes are not supported on RLV-enabled tables.
 - Foreign key constraints are not supported on RLV-enabled tables or across a combination of RLV-enabled and traditional tables.
-

9. (For system store only) On the Primary Key Constraints page, enter primary key constraint and cluster primary key information. Default is to create a primary key constraint but not a clustered primary key.
10. (For system store only) Click **Next**.
11. (For system store only) On the Free Space page, enter free space information. Default is to reserve 200 bytes for each table page or accept the defaults
12. Click **Next**.
13. On the Columns page, each row in the Column Definitions table corresponds to a column. Click **New** to add column definitions for the table.
14. Follow the Create Column wizard prompts.
 - a) On the Column Name page, specify:

Option	Description
Column Name	Name of the column.
Is the column a primary key?	Indicates you are using the column as a primary key (default).

- b) Click **Next**.
 - c) On the Data Type page, specify:

Option	Description
Built-in type	<p>(Default) Choose a predefined data type for the column. Integers, character strings, and dates are examples of predefined data types. For some of these types, you can specify size and scale.</p> <ul style="list-style-type: none"> • Size — Length of string columns, or the total number of digits to the left and right of the decimal point in the result of any decimal arithmetic for numeric columns. For numeric columns, the size is also called the PRECISION value. • Scale — Minimum number of digits after the decimal point when an arithmetic result is truncated to the maximum PRECISION value. • Units — Unit corresponding to the data type's size. Possible units include: bits, bytes, characters, or digits. For CHAR and VARCHAR data types, you can specify the unit as bytes or characters. • Compress values — Not available for all built-in types) Select to compress column values. If a column is compressed, database server activities such as indexing, data comparisons, and statistics generation may be slightly slower if they involve the compressed column because the values must be compressed when written, and decompressed when read. • Maintain BLOB indexes for large values — (Available for character, binary, and bit types only) Maintain BLOB indexes for large values.
Domain	Choose a domain. A domain is a named combination of built-in data types, default value, check condition, and nullability.

d) Click **Next**.

e) On the Value page, specify:

Option	Description
No default or computed value	(Default) Select this option if the column is not a computed value and has no default value.

Option	Description
Default Value	<p>Select this option if the column has a default value. If the column is based on a domain, this setting inherits the domain's default value (if any), but you can override the value for the column. Choosing the Default value option enables the User-defined and System-defined options.</p> <ul style="list-style-type: none"> • User-defined — Type a custom value (string, number, or other expression) for the default value. If you have based the column on a domain, you can retain the domain's default value (if any), or override it for the column • Literal string — Specify whether the default value for the column should be treated as a literal string. By default, this option is selected for character columns and domains with a character base type. You do not need to enclose default text in single quotes, and escape embedded single quotes or backslashes in the string. • System-defined — Lets you select a predefined value (for example, current date) for the default value. Select a value. If you have based the column on a domain, you can retain the domain's default value (if any) or override it for the column. • Select Autoincrement or Global Autoincrement from the list. • If you select global autoincrement, the domain of values for that column is partitioned. Each partition contains the same number of values. For example, if you set the partition size for an integer column in a database to 1000, one partition extends from 1001 to 2000, the next from 2001 to 3000, and so on.
Computed Value	<p>Define a computed value for the column. A computed column derives its values from calculations of values in other columns. Type an expression in the text box to describe the relationship between the other columns and the value that appears in the computed column.</p>

f) Click **Next**.

g) On the Constraints page, specify:

Option	Description
Values can be null	(Default) Select this option if null values are allowed in the column. If the column is based on a domain, you can retain the domain's nullability or override it for the column.
Values cannot be null	Select this option to allow duplicate values, but not allow null values in this column.

Option	Description
Values cannot be null and must be unique	Select this option if values in the column cannot be null and must be unique.

h) Click **Next**.

i) (For IQ store only) On the Placement page, specify:

Field	Description
Select the placement details for this column	From the list, select the dbspace.

j) (For IQ store only) Click **Next**.

k) (Optional) On the Comment page, specify:

Option	Description
What would you like the comment for this column to be?	Add a descriptive comment for the column. Comments help you organize your database.

l) Click **Finish** to create the column.

m) Repeat steps 14 on page 468 and 14.1 to create additional columns. When all columns are added, click **Next**.

15. (Optional) On the Partitions page, click **New**.

16. Follow the Create Partition wizard prompts.

a) On the Partition Type tab, specify a hash partition:

Option	Description
What type of partition do you want to create?	Select Hash, Range, or Hash-Range.

a) Click **Next**.

b) On the Partition Key page, specify one or more columns.

Option	Description
Which column do you want to include in the partition key?	<p>Select one (for range partition key) or more table columns and click Add.</p> <p>A partition key cannot contain LOB, binary, varbinary, bit, float, double, or real data, or any char or varchar column with a length that exceeds 255 bytes.</p> <p>Hash partition keys are restricted to a maximum of 8 columns with a declared column width of 5300 bytes or less.</p>

c) (For range or hash-range partition only) Click **Next**.

d) (For hash-range partition only) On the Subpartition page, specify a column:

Option	Description
Which column do you want to include in the subpartition key?	<p>Select a table column and click Add</p> <p>A partition key cannot contain LOB, binary, varbinary, bit, float, double, or real data, or any char or varchar column over 255 bytes long.</p>

- e) (For hash-range partitions only) Click **Next**.
- f) (For hash-range partitions only) On the Subpartitions page, specify the range partition definition:

Option	Description
Specify the name, value and dbspace for the range subpartition.	<ul style="list-style-type: none"> • Name — Enter a descriptive name for the partition. • Constraint — Less than or equal (\leq) is the only constraint currently supported. • Value — Enter the upper limit value of the partition. • Dbspace — Select the dbspace for the partition from the pull-down.

- g) (For hash-range partitions only) On the Columns page, click **Add** if you want to store the data for any individual columns in separate dbspaces from the partition. Otherwise continue to the Comment page.

If you click **Add**, the Specify Dbspace for a Partition Column page appears.

- h) (For hash-range partitions only) Choose the column, partition, and dbspace from the pull-down and click **OK**.
- i) (For hash-range partitions only) When you have specified all the desired columns, continue to the Comment page.
- j) (For range partition only) On the Partitions page, click **Add**.

The Define a Partition page appears.

- k) (For range partitions only) On the Define a Partition page, specify the range partition definition:

Option	Description
Specify the name, value and dbspace for the range partition.	<ul style="list-style-type: none"> • Name — Enter a descriptive name for the partition. • Constraint — Less than or equal (\leq) is the only constraint currently supported. • Value — Enter the upper limit value of the partition. • Dbspace — Select the dbspace for the partition from the pull-down.

- l) (For range partitions only) On the Columns page, click **Add** if you want to store the data for any individual columns in separate dbspaces from the partition. Otherwise, continue to the Comment page.
 - m) (For range partitions only) If you click Add, the Specify Dspace for a Partition Column page appears.
 - n) (For range partitions only) Choose the column, partition, and dspace from the pull-down and click **OK**.
 - o) (For range partitions only) When you have specified all the columns desired, continue to the Comment page.
17. (Optional) On the Comment page, enter a comment about the table.
18. Click **Finish**.

See also

- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Global Temporary Table

Add a global temporary table to the database. A global temporary table definition is kept in the database permanently. (The data disappears when you close the connection.)

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Global temporary table to be owned by self:</p> <ul style="list-style-type: none"> Requires RESOURCE authority with CREATE permission on the main store dbspace in which the table is created. <p>Global temporary table to be owned by any user – Requires DBA authority.</p>
SAP Sybase IQ 16.0	<p>Global temporary table to be owned by self:</p> <ul style="list-style-type: none"> Requires CREATE TABLE system privilege. <p>Global temporary table to be owned by any user – Requires one of:</p> <ul style="list-style-type: none"> CREATE ANY TABLE system privilege. CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

Altering or creating global tables can interfere with other users of the database.

For large tables, modifying an existing table or creating a new table can be a time-consuming operation. The internal **CREATE TABLE** statement delays execution of other processes until the statement completes. Although you modify tables while other connections are active, you cannot execute them while any other connection uses the table to be altered. Modifying a table excludes other requests referencing the table being offered while the internal **ALTER TABLE** statement processes.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables > Global Temporary Tables**.
3. Click the arrow next to **Global Temporary Tables** and select **New**.
The Create Global Temporary Table wizard appears.
4. On the Welcome page, specify

Option	Description
Select a resource for which the table will be created	From the list, select the resource for which the table will be created.
What do you want to name the table?	Enter a unique name for the new table; maximum of 128 characters.
Which user do you want to own the table?	From the list, select the user to own the table.

5. Click **Next**.
6. On the Type page, specify the type of global temporary table to create. For transactional (default), specify whether the rows are deleted (default) or preserved when a commit occurs. Non-transactional global temporary tables are not affected by commit or rollback operations and can provide performance improvements in some circumstances since operations on the table do not cause entries to be made in the rollback log.
7. Click **Next**.
8. On the Columns page, each row in the Column Definitions table corresponds to a column. Click **New** to add column definitions for the table.
9. Follow the Create Column wizard prompts.
 - a) On the Column Name page, specify:

Option	Description
Column Name	Name of the column.
Is the column a primary key?	Indicates you are using the column as a primary key (default).

- b) Click **Next**.
 - c) On the Data Type page, specify:

Option	Description
Built-in type	<p>(Default) Choose a predefined data type for the column. Integers, character strings, and dates are examples of predefined data types. For some of these types, you can specify size and scale.</p> <ul style="list-style-type: none"> • Size — Length of string columns, or the total number of digits to the left and right of the decimal point in the result of any decimal arithmetic for numeric columns. For numeric columns, the size is also called the PRECISION value. • Scale — Minimum number of digits after the decimal point when an arithmetic result is truncated to the maximum PRECISION value. • Units — Unit corresponding to the data type's size. Possible units include: bits, bytes, characters, or digits. For CHAR and VARCHAR data types, you can specify the unit as bytes or characters. • Compress values — Not available for all built-in types) Select to compress column values. If a column is compressed, database server activities such as indexing, data comparisons, and statistics generation may be slightly slower if they involve the compressed column because the values must be compressed when written, and decompressed when read. • Maintain BLOB indexes for large values — (Available for character, binary, and bit types only) Maintain BLOB indexes for large values.
Domain	Choose a domain. A domain is a named combination of built-in data types, default value, check condition, and nullability.

d) Click **Next**.

e) On the Value page, specify:

Field	Description
No default or computed value	(Default) Select this option if the column is not a computed value and has no default value.

Field	Description
Default value	<p>Select this option if the column has a default value. If the column is based on a domain, this setting inherits the domain's default value (if any), but you can override the value for the column. Choosing the Default value option enables the User-defined and System-defined options.</p> <ul style="list-style-type: none"> • User-defined — Type a custom value (string, number, or other expression) for the default value. If you have based the column on a domain, you can retain the domain's default value (if any), or override it for the column. • Literal string — Specify whether the default value for the column should be treated as a literal string. By default, this option is selected for character columns and domains with a character base type. You do not need to enclose default text in single quotes, and escape embedded single quotes or backslashes in the string. • System-defined — Lets you select a predefined value (for example, current date) for the default value. Select a value. If you have based the column on a domain, you can retain the domain's default value (if any) or override it for the column. <ul style="list-style-type: none"> • Select Autoincrement or Global Autoincrement from the list. • If you select global autoincrement, the domain of values for that column is partitioned. Each partition contains the same number of values. For example, if you set the partition size for an integer column in a database to 1000, one partition extends from 1001 to 2000, the next from 2001 to 3000, and so on.
Computed Value	<p>Define a computed value for the column. A computed column derives its values from calculations of values in other columns. Type an expression in the text box to describe the relationship between the other columns and the value that appears in the computed column.</p>

f) Click **Next**.

g) On the Constraints page, specify:

Field	Description
Values can be null	(Default) Select this option if null values are allowed in the column. If the column is based on a domain, you can retain the domain's nullability or override it for the column.
Values cannot be null	Select this option to allow duplicate values, but not allow null values in this column.

Field	Description
Values cannot be null and must be unique	Select this option if values in the column cannot be null and must be unique.

h) Click **Next**.

i) (Optional) On the Comment page, specify:

Field	Description
What would you like the comment for this column to be?	Add a descriptive comment for the column. Comments help you organize your database.

j) Click **Finish** to create the column.

k) Repeat steps 9 on page 475 and 9.j to create additional columns. When all columns are added, click **Next**

10. (Optional) On the Comment page, enter a comment about the global temporary table.

11. Click **Finish** to create the column.

See also

- *Creating a Table* on page 466
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617

- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Proxy Table

A proxy table is a locally named alias, displayed as a table, that points to a remote object such as an entire table, a view, a materialized view, or a set of remote table columns. Before you can map remote objects to a local proxy table, you must define the remote server where the remote object is located.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Proxy table to be owned by self: <ul style="list-style-type: none"> • Requires RESOURCE authority with CREATE permission on the main store dbspace in which the table is created. Proxy table to be owned by any user – Requires DBA authority.
SAP Sybase IQ 16.0	Proxy table to be owned by self – Requires CREATE PROXY TABLE system privilege. Proxy table to be owned by any user – Requires one of: <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege • CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- Before you can map remote objects to a local proxy table, you must define the remote server where the remote object is located.

Task

You can use a proxy table to access any object (including tables, views, and materialized views) that the remote database exports as a candidate for a proxy table. Location transparency of remote data is enabled by creating a local proxy table that maps to the remote object.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables > Proxy Tables**.
3. Click the arrow next to **Proxy Tables** and select **New**.
The Create Proxy Table wizard appears.
4. On the Server and User page, specify

Option	Description
Select a resource for which the proxy table will be created	From the list, select the resource for which the proxy table will be created.
To which remote server do you want to create the proxy table?	From the list, select the remote server.
Which user will own the proxy table?	From the list, select the user to own the table. Default is dba user.
(Optional) Remote database name	Specify the name of the remote database associated with the remote server. Note: You specify a remote database on which your remote login has system privileges.

5. Click **Next**.
6. On the Table Selection page, specify:

Option	Description
Which table do you want to use for this proxy table?	From the list, select the object on the remote server (table / view / materialized view) that will be used as the target of the local proxy.
What do you want to name the new proxy table.	Enter a unique name for the new proxy table. You cannot create two tables with the same name under the same user ID. The default name of the proxy table is the name of the object on the remote server. However, this may not be a unique name to your user ID.

7. Click **Next**.
8. On the Column Selection page, select the columns to be used in the proxy table. Default is to use all columns.
9. Click **Next**.
10. On the Comments page, add a descriptive comment for the proxy table. Comments help you organize the database.
11. Click **Finish**.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Viewing Table Data in the Execute SQL Window* on page 481

- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing Table Data in the Execute SQL Window

Execute a **SELECT * FROM** query and display contents of the table, global temporary table or proxy table in the query results pane of the Execute SQL window.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of the following to enable menu option:</p> <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. • You own the table. <p>Queries execute with user's current permissions.</p>

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>Requires one of the following to enable menu option:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Queries execute with user's current privileges.</p>

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, **Global Temporary Tables**, or **Proxy Tables**.
4. In the right pane, select a table.
5. Click the drop-down arrow that appears next to the table name and select **View Data in SQL**.
A **SELECT * FROM <table>** query executes.
6. (Optional) Modify the SQL statement and click **Execute** to display different data in the table.
7. Click **Close** to close the Execute SQL view.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501

- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Table

Delete a table, global temporary table or proxy table from the database.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY TABLE system privilege. • DROP ANY OBJECT system privilege. • You own the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, **Global Temporary Tables**, or **Proxy Tables**.
4. Select one or more tables from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Use **Shift-click** or **Control-click** to select multiple tables.

5. Click **Yes** to confirm deletion.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Table DDL Commands

Display the data description language SQL code for adding a table, global temporary table or proxy table to a dbspace. The DDL can be a useful reference and training tool.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	None required.

Database Version	Table Privileges
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables, Global Temporary Tables, or Proxy Tables**.
4. Select one or more tables from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Use **Shift-click** or **Control-click** to select multiple tables.

The DDL view shows the SQL code used to add the selected table to the dbspace.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556

- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Moving a Table to Another Dbspace

You can move the table from the current dbspace to another dbspace. This feature is available only for tables in the IQ main store.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• SPACE ADMIN authority.• You own the table and have CREATE permission on the target dbspace.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• ALTER ANY TABLE system privilege.• ALTER ANY OBJECT system privilege.• MANAGE ANY DBSPACE system privilege.• ALTER permission on the table and CREATE permission on the target dbspace.• You own the table and have CREATE permission on the target dbspace.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The table is an SAP Sybase IQ base table (not an IQ catalog store table, global temporary table, or proxy table).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables > Tables**.
3. Select one or more tables from the right pane and either:

- Click the arrow to the right of the name and select **Move**, or
- From the Administration Console menu bar, select **Resource > Move**.

Use **Shift-click** or **Control-click** to select multiple tables.

4. In the Move Object Dialog view, click the arrow and select the new dbspace.
5. Click **OK** to execute the move.
6. Click **OK** to save the change and close the Move Object Dialog view.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Validating a System Store Table

Check the validity of a system store (IQ catalog store) table. This feature is available only for tables in the system store.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • VALIDATE authority.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The table is an IQ catalog store table (not an IQ base table, global temporary table, or proxy table)

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables > Tables**.
3. Select one or more tables from the right pane and either:
 - Click the arrow to the right of the name and select **Validate**, or
 - From the Administration Console menu bar, select **Resource > Validate**.

Use **Shift-click** or **Control-click** to select multiple tables.

The Validate Tables view appears indicating the validation status of each selected table.

If the table does not validate, try one of these solutions:

- Drop all the indexes and keys on a table and recreate them. Recreate any foreign keys to the table.
 - If you suspect a particular index, you can execute an **ALTER INDEX ... REBUILD** statement to rebuild the corrupted index.
 - Unload and reload your entire database.
4. Click **OK**.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474

- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Executing a SQL Query* on page 324
- *Authenticating a Login Account for a Managed Resource* on page 282

Setting the Primary Key

Set the primary key to prohibit two or more rows in the table from having identical values for a column or set of columns. You can set the primary key on base tables and global temporary tables only.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER and REFERENCE permission on the table. • You own the table.

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>To create a new or modify an existing primary key - Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace where the table resides. • ALTER and REFERENCE permission on the table. • You own the table. <p>To modify the name only of an existing primary key, requires ALTER ANY INDEX system privilege.</p>

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Set Primary Key**, or
 - From the Administration Console menu bar, select **Resource > Set Primary Key**.

The Set Primary Key wizard appears.

5. On the Constraint Name page of the wizard, specify the primary key name and click **Next**.

If the table does not already have a primary key, the primary key name is optional.

6. On the Columns page, specify:

Option	Description
Add Asc. >>	Moves columns from the Available Columns pane to the Selected Columns pane, in ascending order.
Add Desc. >>	(IQ catalog store (system store) tables only.) Moves columns from the Available Columns pane to the Selected Columns pane, in descending order.
<< Remove	Moves columns from the Selected Columns pane to the Available Columns pane.

Select columns that do not allow NULL values.

7. Click **Next**.
8. (System store (IQ catalog store) tables only) On the clustered index page, specify:

Option	Description
Create a clustered primary key	Select if you want to make the primary key's underlying index a clustered index. Clustered indexes can improve performance.

9. Click **Next**.
10. On the Comment page, add an optional, descriptive comment. Comments help you organize your database.
11. Click **Finish** to close the Set Primary Key wizard.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Setting a Clustered Index

Set a clustered index on a system store (IQ catalog store) table. Using a clustered index increases the chance that two rows from adjacent index entries will appear on the same page in the database. This strategy can lead to performance benefits by reducing the number of times a table page needs to be read into the buffer pool.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • ALTER and REFERENCE permission on the table. • You own the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The table exists in the system store.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables > Tables**.
3. Select a catalog store table from the right pane and either:
 - Click the arrow to the right of the name and select **Set Clustered Index**, or
 - From the Administration Console menu bar, select **Resource > Set Clustered Index**.

The Set Clustered Index Wizard appears.

4. Select an index in the list of indexes. Set the clustered index:

Field	Description
Specify an index on this table to be clustered	Select the check box to cluster the list of indexes. Any previously clustered indexes in the list will no longer be clustered. If you clear the check box, the currently clustered index will be unclustered.

5. Click **OK**.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Merging Table Data from RLV Store with IQ Main Store

Read-write data from a table enabled with row-level versioning (RLV) is housed in the RLV store, and periodically merged automatically with the table's data in the IQ main store.

However, you can explicitly merge this RLV-enabled table data from the RLV store with the IQ main store data.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• ALTER ANY TABLE system privilege.• ALTER ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The RLV store dbspace exists.
- The data is stored in a single RLV-enabled table.
- Only IQ base tables are supported in the RLV store: catalog, temporary and global temporary tables are not supported.
- LONG VARBINARY (LOB) and LONG VARCHAR data types are not supported on RLV-enabled tables.
- TEXT and WORD indexes are not supported on RLV-enabled tables.
- Foreign key constraints are not supported on RLV-enabled tables or across a combination of RLV-enabled and traditional tables.

Task

An RLV-enabled table uses row-level versioning so multiple writer connections can make simultaneous updates to different rows of the same table.

The RLV store contains all rows of a RLV-enabled table which have been inserted or updated since the last merge.

RLV merge is the process where the latest committed data from the RLV store is written to the IQ main store to create a new main store table-level snapshot version.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**.
4. In the right pane, select an RLV-enabled table.
5. Click the drop-down arrow that appears next to the table name and select **Merge RLV**. The menu item is disabled for tables that are not RLV-enabled.

6. In the Merge RLV dialog, click **OK**.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Calculating the Number of Rows in a Table

Calculate an accurate row count for a base or proxy table.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. • You own the table.

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, click **Miscellaneous**.
6. Adjust the calculation values as needed.
7. Click **Calculate**.
Calculation time depends on the size of the table. The number of rows appears beside **Number of rows**:. The number of columns appears beside **Number of Columns**.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Moving Table Objects to Another Dbspace* on page 497

- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Moving Table Objects to Another Dbspace

You can move SAP Sybase IQ table objects—including indexes, columns, and partitions—from the current dbspace to another dbspace. This feature is available only for tables in the IQ main store.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires CREATE permission on the target dbspace. Also requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the table. • You own the table.
SAP Sybase IQ 16.0	Requires CREATE permission on the target dbspace. Also requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • Requires MANAGE ANY DBSPACE system privilege. • You own the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The table is a base table (not a catalog store table, global temporary table, or proxy table).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables > Tables**.
3. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

4. In the left pane, select **Table Objects**.
5. In the right pane, select an object (index, column, partition) and click **Move**.
6. In the Move Object Dialog view, click the arrow and select the new dbspace.
7. Click **OK** to execute the move.
8. Click **OK** to save the change and close the Table Properties view.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586

- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Enabling or Disabling Row-Level Versioning in a Table

You can set a base table to use row-level versioning (RLV) in order to track row changes for read-write transactions.

Prerequisites

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The RLV store dbspace exists.
- You have a simplex configuration of SAP Sybase IQ 16.0.
- Only IQ base tables are supported in the RLV store: catalog, temporary and global temporary tables are not supported.
- LONG VARBINARY (LOB) and LONG VARCHAR data types are not supported on RLV-enabled tables.
- TEXT and WORD indexes are not supported on RLV-enabled tables.
- Foreign key constraints are not supported on RLV-enabled tables or across a combination of RLV-enabled and traditional tables.

Task

If your implementation uses the in-memory RLV store, you can enable row-level snapshot versioning so multiple connections can make concurrent updates to different rows of the same table.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**.
4. In the right pane, select a table, click the drop-down arrow that appears next to the table name and select **Properties**.

5. Select **Row-level Versioning**.
6. Select the **Enabled** checkbox if you want the table to use row-level versioning to track row changes for read-write transactions on the table. The RLV dbspace must exist to enable RLV on tables
Or, deselect the **Enabled** checkbox to disable row-level versioning. .
7. Click **OK**.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Base Table Properties

Display or change the properties of the selected IQ store (main store) or IQ system store (catalog store) base table.

Prerequisites

Note: The system privileges and permissions required vary by task. Unless otherwise indicated, the following system privileges and permissions apply.

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any property page of a base table owned by self – None required.</p> <p>View any property page of a base table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. • You own the table. <p>Modify any property on the General page requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table. <p>Modify any property on the Miscellaneous page requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603 • <i>Table Trigger Privilege Summary</i> on page 615 • <i>Table Partition Privilege Summary</i> on page 639

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>View any property page of a base table owned by self – None required.</p> <p>View any property page of a base table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify the table name on the General page – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • You own the table. <p>Use the Calculate button on the Miscellaneous page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify any other property on the Miscellaneous page for an IQ catalog (system) store table – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table. • You own the table. <p>Modify a comment on the General page – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege • ALTER ANY TABLE system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603 • <i>Table Trigger Privilege Summary</i> on page 615

Database Version	Table Privileges
	<ul style="list-style-type: none"> • <i>Table Partition Privilege Summary</i> on page 639

- The SAP Sybase IQ resource is authenticated and running.
- (Modifying properties only) In a multiplex configuration, the coordinator node is running.
- (Enabling RLV in tables) The RLV store dbspace exists. (Row-level versioning can only be enabled in base tables in the IQ 16.0 main store for a simplex resource.)
- (Partitioning tables) The table to be partitioned is empty.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**.
4. In the right pane, select a table, click the drop-down arrow that appears next to the table name and select **Properties**.
5. View or modify table properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – Table identifier.</p> <p>Owner – (Read-only) Database user who owns the table.</p> <p>Type – (Read-only) Type of table - base table or global temporary table.</p> <p>Dbspace – (Read-only) The dbspace in which the table is located.</p> <p>Comment – Text description of the table. For example, describe the table's purpose in the system.</p>
Columns	See <i>Table Columns</i> on page 528.
Permissions	<p>(Base tables and global temporary tables only.)</p> <p>See <i>Table Permissions</i> on page 543.</p>

Area	Description
Placement (Read-only)	<p>Name – Name of the first table object.</p> <p>Dbospace – Dbospace occupied by the object.</p> <p>Size – Size of the object.</p> <p>% File – Percentage of the file used by this object.</p> <p>First Block – First block used by this object.</p> <p>Last Block – Last block used by this object.</p>
Constraints	See <i>Table Constraints</i> on page 556.
Referencing Constraints	See <i>Table Constraints</i> on page 556.
Indexes	See <i>Table Indexes</i> on page 586.
Text Indexes	See <i>Table Indexes</i> on page 586.
Triggers	<p>(System store tables only.)</p> <p>See <i>Table Triggers</i> on page 606.</p>
Partitions	<p>(Base tables only.)</p> <p>See <i>Table Partitions</i> on page 617.</p>
Row-Level Versioning	Select the Enabled checkbox if you want the table to use row-level versioning to track row changes for read-write transactions on the table. Deselect the checkbox to disable row-level versioning. The RLV dbospace must exist before you can enable RLV on tables.
Dependent Views (Read-only)	<p>Name – Name of the dependent view.</p> <p>Owner – Owner of the dependent view.</p> <p>View Type – Indicates if the view is a regular view or materialized view.</p> <p>Referenced Column – List of referenced table columns in the view.</p> <p>Dependency Type – Indicates if the dependency is direct or indirect.</p>

Area	Description
Table Objects	<p>Name – Name of the table object.</p> <p>Type – Type of table object. For example, "column".</p> <p>Partitions – Partition where this column's data is stored.</p> <p>Dbspace – Dbspace where the partition (storing the column data) resides.</p> <p>See <i>Moving Table Objects to Another Dbspace</i> on page 497.</p>
Data (Read-only)	<p>Note: For 15.3 and 15.4, requires SELECT permission on the table to view data. For 16.0, requires the SELECT ANY TABLE system privilege to view data.</p> <p>Displays the first 500 rows of data.</p>
Miscellaneous Read-only)	<p>Number of rows – Approximate number of rows in the table. To update this value, click Calculate.</p> <p>Calculate – (System store tables only.) Calculates the number of rows in the table.</p> <p>Number of Columns – (System store tables only.) Number of columns in the table.</p> <p>Time Created – (System store tables only.) Date and time the table was created.</p> <p>Time Updated – (System store tables only.) Date and time the table was last updated.</p> <p>Reserved space for each table page – (Catalog store tables only.)</p> <p>Table is replicating data – (Catalog store tables only.)</p>

6. Click **OK**.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486

- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Viewing or Modifying Table Index Properties* on page 599
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Global Temporary Table Properties

Display or change the properties of the selected global temporary table.

Prerequisites

Note: The system privileges and permissions required vary by task. Unless otherwise indicated, the following system privileges and permissions apply.

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any property page of a global temporary table owned by self – None required.</p> <p>View any property page of a global temporary table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. • You own the table. <p>Modify any property on the General page requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table. <p>Modify any property on the Miscellaneous page requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603 • <i>Table Trigger Privilege Summary</i> on page 615

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>View any property page of a global temporary table owned by self – None required.</p> <p>View any property page of a global temporary table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify the table name on the General page – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • You own the table. <p>Use the Calculate button on the Miscellaneous page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify any other property on the Miscellaneous page for an IQ catalog (system) store table – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table. • You own the table. <p>Modify a comment on the General page – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege • ALTER ANY TABLE system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603

Database Version	Table Privileges
	<ul style="list-style-type: none"> • <i>Table Trigger Privilege Summary</i> on page 615

- The SAP Sybase IQ resource is authenticated and running.
- (Modifying properties only) In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Global Temporary Tables**.
4. In the right pane, select a table, click the drop-down arrow that appears next to the table name and select **Properties**.
5. View or modify table properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – Table identifier.</p> <p>Owner – (Read-only) Database user who owns the table.</p> <p>Type – (Read-only) Type of table - base table or global temporary table.</p> <p>Commit Action – (Read-only) Identifies if the table is Transactional or Non-transactional.</p> <p>Comment – Text description of the table. For example, describe the table's purpose in the system.</p>
Columns	See <i>Table Columns</i> on page 528.
Permissions	See <i>Table Permissions</i> on page 543.

Area	Description
Placement (Read-only)	<p>Name – Name of the first table object.</p> <p>Dbpace – Dbpace occupied by the object.</p> <p>Size – Size of the object.</p> <p>% File – Percentage of the file used by this object.</p> <p>First Block – First block used by this object.</p> <p>Last Block – Last block used by this object.</p>
Constraints	See <i>Table Constraints</i> on page 556.
Referencing Constraints	See <i>Table Constraints</i> on page 556.
Indexes	See <i>Table Indexes</i> on page 586.
Triggers	See <i>Table Triggers</i> on page 606.
Dependent Views (Read-only)	<p>Name – Name of the dependent view.</p> <p>Owner – Owner of the dependent view.</p> <p>View Type – Indicates if the view is a regular view or materialized view.</p> <p>Referenced Column – List of referenced table columns in the view.</p> <p>Dependency Type – Indicates if the dependency is direct or indirect.</p>
Table Objects	<p>Name – Name of the table object.</p> <p>Type – Type of table object. For example, "column".</p> <p>Partitions – Partition where this column's data is stored.</p> <p>Dbpace – Dbpace where the partition (storing the column data) resides.</p> <p>See <i>Moving Table Objects to Another Dbpace</i> on page 497.</p>
Data (Read-only)	<p>Note: For 15.3 and 15.4, requires SELECT permission on the table to view data. For 16.0, requires the SELECT ANY TABLE system privilege to view data.</p> <p>Displays the first 500 rows of data.</p>

Area	Description
Miscellaneous Read-only)	<p>Number of rows – Approximate number of rows in the table. To update this value, click Calculate.</p> <p>Calculate – Calculates the number of rows in the table.</p> <p>Number of Columns – Number of columns in the table.</p> <p>Time Created – Date and time the table was created.</p> <p>Time Updated – Date and time the table was last updated.</p>

6. Click **OK**.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing and Modifying Proxy Table Properties

Display the properties of the selected proxy table. Only the **Comment** property is editable.

Prerequisites

Note: The system privileges and permissions required vary by task. Unless otherwise indicated, the following system privileges and permissions apply.

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any property page of a proxy table owned by self – None required except for Data page, which requires SELECT permission on the base table on the remote server.</p> <p>View any properties of a proxy table owned by any user – None required except for Data page, which requires:</p> <ul style="list-style-type: none"> • SELECT permission on the base table on the remote server. • Also requires one of: <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. <p>Modify any property on the General or Miscellaneous page requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Trigger Privilege Summary</i> on page 615

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>View any property page of a proxy table owned by self – None required except for Data page, which requires SELECT permission on the base table on the remote server.</p> <p>View any property page of a proxy table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the proxy table. • SELECT permission on the base table. • You own the table. <p>Use the Calculate button on the Miscellaneous page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the proxy table. • You own the table. <p>Modify a comment on the General page requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Trigger Privilege Summary</i> on page 615

- The SAP Sybase IQ resource is authenticated and running.
- (Modifying properties only) In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Proxy Tables**.
4. In the right pane, select a table, click the drop-down arrow that appears next to the table name and select **Properties**.

5. View or modify table properties.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) Table identifier.</p> <p>Owner – (Read-only) Database user who owns the table.</p> <p>Remote location – (Read-only) Shows the location of the remote table that the proxy table is based on.</p> <p>Comment – Text description of the table. For example, describe the table's purpose in the system.</p>
Columns	See <i>Table Columns</i> on page 528.
Triggers	See <i>Table Triggers</i> on page 606.
Data (Read-only)	<p>Requires SELECT permission on the base table on the remote server.</p> <hr/> <p>Note: For 15.3 and 15.4, requires SELECT permission on the table to view data. For 16.0, requires the SELECT ANY TABLE ROLE system privilege to view data.</p> <hr/> <p>Displays the first 500 rows of data.</p>
Miscellaneous Read-only)	<p>Number of rows – Approximate number of rows in the table. To update this value, click Calculate.</p> <p>Calculate – Calculates the number of rows in the table.</p> <p>Number of Columns – Number of columns in the table.</p> <p>Time Created – Date and time the table was created.</p> <p>Time Updated – Date and time the table was last updated.</p>

6. Click **OK**.**See also**

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483

- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617
- *Authenticating a Login Account for a Managed Resource* on page 282

Table Privilege Summary

A list of the system privileges and object permissions required to complete the various table tasks.

Creating a Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Base table to be owned by self:</p> <ul style="list-style-type: none"> • Requires RESOURCE authority with CREATE permission on the main store dbspace in which the table is created. <p>Base table to be owned by any user – Requires DBA authority.</p>

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>Base table to be owned by self –</p> <ul style="list-style-type: none"> Requires CREATE permission on the dbspace where the table is created. Also requires one of: <ul style="list-style-type: none"> CREATE TABLE system privilege. CREATE ANY OBJECT system privilege <p>Base table to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE permission on the dbspace where the table is created. Also requires one of: <ul style="list-style-type: none"> CREATE ANY TABLE system privilege. CREATE ANY OBJECT system privilege

Creating a Global Temporary Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Global temporary table to be owned by self:</p> <ul style="list-style-type: none"> Requires RESOURCE authority with CREATE permission on the main store dbspace in which the table is created. <p>Global temporary table to be owned by any user – Requires DBA authority.</p>
SAP Sybase IQ 16.0	<p>Global temporary table to be owned by self:</p> <ul style="list-style-type: none"> Requires CREATE TABLE system privilege. <p>Global temporary table to be owned by any user – Requires one of:</p> <ul style="list-style-type: none"> CREATE ANY TABLE system privilege. CREATE ANY OBJECT system privilege.

Creating a Proxy Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Proxy table to be owned by self:</p> <ul style="list-style-type: none"> Requires RESOURCE authority with CREATE permission on the main store dbspace in which the table is created. <p>Proxy table to be owned by any user – Requires DBA authority.</p>
SAP Sybase IQ 16.0	<p>Proxy table to be owned by self – Requires CREATE PROXY TABLE system privilege.</p> <p>Proxy table to be owned by any user – Requires one of:</p> <ul style="list-style-type: none"> CREATE ANY TABLE system privilege CREATE ANY OBJECT system privilege.

Viewing Table Data in the Execute SQL Windows

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of the following to enable menu option:</p> <ul style="list-style-type: none"> DBA authority. SELECT permission on the table. You own the table. <p>Queries execute with user's current permissions.</p>
SAP Sybase IQ 16.0	<p>Requires one of the following to enable menu option:</p> <ul style="list-style-type: none"> SELECT ANY TABLE system privilege. SELECT permission on the table. You own the table. <p>Queries execute with user's current privileges.</p>

Deleting a Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> DBA authority. You own the table.

Database Version	Table Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY TABLE system privilege. • DROP ANY OBJECT system privilege. • You own the table.

Generating Table DDL Commands

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Moving a Table to Another Dbspace

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority. • You own the table and have CREATE permission on the target dbspace.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • ALTER permission on the table and CREATE permission on the target dbspace. • You own the table and have CREATE permission on the target dbspace.

Validating a System Store Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • VALIDATE authority.

Database Version	Table Privileges
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

Setting the Primary Key

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER and REFERENCE permission on the table. • You own the table.
SAP Sybase IQ 16.0	To create a new or modify an existing primary key - Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace where the table resides. • ALTER and REFERENCE permission on the table. • You own the table. <p>To modify the name only of an existing primary key, requires ALTER ANY INDEX system privilege.</p>

Setting a Clustered Index

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • ALTER and REFERENCE permission on the table. • You own the table.

Moving Table Data from RLV Store to IQ Main Store

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> ALTER ANY TABLE system privilege. ALTER ANY OBJECT system privilege.

Calculating the Number of Rows in a Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> DBA authority. SELECT permission on the table. You own the table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> SELECT ANY TABLE system privilege. SELECT permission on the table. You own the table.

Moving Table Objects to Another Dbspace

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Requires CREATE permission on the target dbspace. Also requires one of: <ul style="list-style-type: none"> DBA authority. RESOURCE authority with ALTER permission on the table. You own the table.

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>Requires CREATE permission on the target dbspace.</p> <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • Requires MANAGE ANY DBSPACE system privilege. • You own the table.

Enabling Row-Level Versioning in a Table

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege.

Viewing or Modifying Base Table Properties

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any property page of a base table owned by self – None required.</p> <p>View any property page of a base table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. • You own the table. <p>Modify any property on the General page requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table. <p>Modify any property on the Miscellaneous page requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603 • <i>Table Trigger Privilege Summary</i> on page 615 • <i>Table Partition Privilege Summary</i> on page 639

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>View any property page of a base table owned by self – None required.</p> <p>View any property page of a base table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify the table name on the General page – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • You own the table. <p>Use the Calculate button on the Miscellaneous page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify any other property on the Miscellaneous page for an IQ catalog (system) store table – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table. • You own the table. <p>Modify a comment on the General page – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege • ALTER ANY TABLE system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603 • <i>Table Trigger Privilege Summary</i> on page 615

Database Version	Table Privileges
	<ul style="list-style-type: none"> • <i>Table Partition Privilege Summary</i> on page 639

Viewing or Modifying Global Temporary Table Properties

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any property page of a global temporary table owned by self – None required.</p> <p>View any property page of a global temporary table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. • You own the table. <p>Modify any property on the General page requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table. <p>Modify any property on the Miscellaneous page requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603 • <i>Table Trigger Privilege Summary</i> on page 615

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>View any property page of a global temporary table owned by self – None required.</p> <p>View any property page of a global temporary table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify the table name on the General page – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • You own the table. <p>Use the Calculate button on the Miscellaneous page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the table. • You own the table. <p>Modify any other property on the Miscellaneous page for an IQ catalog (system) store table – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table. • You own the table. <p>Modify a comment on the General page – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege • ALTER ANY TABLE system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Permissions Privilege Summary</i> on page 555 • <i>Table Constraints Privilege Summary</i> on page 580 • <i>Table Index Privilege Summary</i> on page 603

Database Version	Table Privileges
	<ul style="list-style-type: none"> • <i>Table Trigger Privilege Summary</i> on page 615

Viewing or Modifying Proxy Table Properties

Database Version	Table Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any property page of a proxy table owned by self – None required except for Data page, which requires SELECT permission on the base table on the remote server.</p> <p>View any properties of a proxy table owned by any user – None required except for Data page, which requires:</p> <ul style="list-style-type: none"> • SELECT permission on the base table on the remote server. • Also requires one of: <ul style="list-style-type: none"> • DBA authority. • SELECT permission on the table. <p>Modify any property on the General or Miscellaneous page requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Trigger Privilege Summary</i> on page 615

Database Version	Table Privileges
SAP Sybase IQ 16.0	<p>View any property page of a proxy table owned by self – None required except for Data page, which requires SELECT permission on the base table on the remote server.</p> <p>View any property page of a proxy table owned by any user – None required except Data page, which requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the proxy table. • SELECT permission on the base table. • You own the table. <p>Use the Calculate button on the Miscellaneous page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the proxy table. • You own the table. <p>Modify a comment on the General page requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>For privileges required to modify other table properties, see:</p> <ul style="list-style-type: none"> • <i>Table Column Privilege Summary</i> on page 540 • <i>Table Trigger Privilege Summary</i> on page 615

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492

- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617

Table Columns

SAP Sybase IQ stores data in columns. Add, modify, and delete table columns.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586

- *Table Triggers* on page 606
- *Table Partitions* on page 617

Adding a Column

Add a column to a base table or global temporary table.

Prerequisites

Database Version	Table Column Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Create a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER permission on the table. • You own the underlying table. <p>Create a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER and REFERENCE permission on the table. • You own the underlying table.
SAP Sybase IQ 16.0	<p>Create a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of the following: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the underlying table. <p>Create a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of the following: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • Both ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, click **Columns** and in the right pane, click **New**
The Create Column Wizard appears.
6. On the Columns Name page, enter a unique name for the column and indicate whether the column is to be a primary key.
7. Click **Next**.
8. On the Data Type page, specify:

Option	Description
Built-in type	<p>Choose a predefined data type for the column. Integers, character strings, and dates are examples of predefined data types. For some of these types, you can specify size and scale.</p> <ul style="list-style-type: none"> • Size – Length of string columns, or the total number of digits to the left and right of the decimal point in the result of any decimal arithmetic for numeric columns. For numeric columns, the size is also called the PRECISION value. • Scale – Minimum number of digits after the decimal point when an arithmetic result is truncated to the maximum PRECISION value. • Units – Unit corresponding to the data type's size. Possible units include: bits, bytes, characters, or digits. For CHAR and VARCHAR data types, you can specify the unit as bytes or characters.
Domain	<p>Choose a domain. A domain is a named combination of built-in data types, default value, check condition, and nullability.</p>

Option	Description
Compress values	Compress column values. If a column is compressed, database server activities such as indexing, data comparisons, and statistics generation may be slightly slower if they involve the compressed column because the values must be compressed when written, and decompressed when read. This option is not available for certain built-in types.
Maintain BLOB indexes for large values	Maintain BLOB indexes for large values. Only character, binary, and bit types support this option.

9. Click Next.

10. On the Value page, specify:

Option	Description
No default or computed value	Select this option if the column is not a computed value and has no default value.
Default Value	<p>Select this option if the column has a default value. If the column is based on a domain, this setting inherits the domain's default value (if any), but you can override the value for the column. Choosing the Default value option enables the User-defined and System-defined options.</p> <ul style="list-style-type: none"> • User-defined – Type a custom value (string, number, or other expression) for the default value. If you have based the column on a domain, you can retain the domain's default value (if any), or override it for the column. • Literal string – Specify whether the default value for the column should be treated as a literal string. By default, this option is selected for character columns and domains with a character base type. You do not need to enclose default text in single quotes, and escape embedded single quotes or backslashes in the string. • System-defined – Lets you select a predefined value (for example, current date) for the default value. Select a value. If you have based the column on a domain, you can retain the domain's default value (if any) or override it for the column.

Option	Description
Partition size	When you select global autoincrement, the domain of values for that column is partitioned. Each partition contains the same number of values. For example, if you set the partition size for an integer column in a database to 1000, one partition extends from 1001 to 2000, the next from 2001 to 3000, and so on.
Computed Value	Define a computed value for the column. A computed column derives its values from calculations of values in other columns. Type an expression in the text box to describe the relationship between the other columns and the value that appears in the computed column.

11. Click **Next**.

12. On the Constraints page, specify:

Option	Description
Values can be null	Select this option if null values are allowed in the column. If the column is based on a domain, you can retain the domain's nullability or override it for the column.
Values cannot be null	Select this option to allow duplicate values, but not allow null values in this column.
Values cannot be null and must be unique	Select this option if values in the column cannot be null and must be unique.

13. Click **Next**.

14. (IQ main store base tables only.) On the Placement page, select a dbspace from the list. Only those dbspaces in read-write mode, and those dbspaces for which the user has permissions, appear in the list.

15. Click **Next**.

16. On the Comment page, add an optional, descriptive comment. Comments help you organize your database.

17. Click **Finish**.

The new column appears in the Column Definitions list.

18. Do one of the following:

- Click **New** to add more columns to the table.
- Click **Apply** to update any column changes to the Table Properties view and remain in the Column Properties view.
- Click **OK** to update any column changes to the Table Properties view and exit the Column Properties view.

Clicking **OK** or **Apply** in the Column Properties view updates any column changes to the Table Properties dialog. It does not save the changes to the database. Your changes are not saved until 19.

19. Click **OK** to save any changes in the Table Properties view to the database.

See also

- *Deleting a Column* on page 533
- *Viewing or Modifying Column Properties* on page 535
- *Table Column Privilege Summary* on page 540
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Column

Delete a column from the table. If the table has only one column, you cannot delete it.

Prerequisites

Database Version	Table Column Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Deleting a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER permission on the table. • You own the underlying table. <p>Deleting a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER and REFERENCE permission on the table. • You own the underlying table.

Database Version	Table Column Privileges
SAP Sybase IQ 16.0	<p>Deleting a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the underlying table. • You own the underlying table. <p>Deleting a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • Both ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

- The table has more than one column.
- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, click **Columns** and in the right pane, select a column and click **Delete**.

Warning! No confirmation prompt appears before the column is deleted.

6. Do one of the following:

- Click **OK** to update the database and permanently remove the column, and exit the Table Properties view.
- Click **Cancel** to cancel the deletion, restore the column, and exit the Table Properties view.

- Click **Apply** to update the database and permanently remove the column, but remain in the Table Properties view.

See also

- *Adding a Column* on page 529
- *Viewing or Modifying Column Properties* on page 535
- *Table Column Privilege Summary* on page 540
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Column Properties

Display or change the properties of the columns of the selected table.

Prerequisites

Database Version	Table Column Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any table column property page – None required.</p> <p>Modify the Primary key property on the General page – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER and REFERENCE permission on the table. • You own the table. <p>Modify any other table column property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table.

Database Version	Table Column Privileges
SAP Sybase IQ 16.0	<p>View any table column property page – None required.</p> <p>Modify the Primary key property on the General page – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • Both ALTER and REFERENCE permission on the table. • You own the table. <p>Modify a table column comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>Modify any other table column property – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table. • You own the table.

- The SAP Sybase IQ resource is authenticated and running.
- (Modifying properties only) In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, or **Global Temporary Tables**.
4. Select a table from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, click **Columns** and in the right pane, select a column and click **Edit**.

The Column Properties view appears.

6. View or modify column properties.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Column Name – Name of the column.</p> <p>Primary key? – Indicates you are using the column as a primary key.</p> <p>Comment – Add a descriptive comment. Comments help you organize your database.</p>
Data Type	<p>Built-in type – Choose a predefined data type for the column. Integers, character strings, and dates are examples of predefined data types. For some of these types, you can specify size and scale.</p> <ul style="list-style-type: none"> • Size – Length of string columns, or the total number of digits to the left and right of the decimal point in the result of any decimal arithmetic for numeric columns. For numeric columns, the size is also called the PRECISION value. • Scale – Minimum number of digits after the decimal point when an arithmetic result is truncated to the maximum PRECISION value. • Units – Unit corresponding to the data type's size. Possible units include: bits, bytes, characters, or digits. For CHAR and VARCHAR data types, you can specify the unit as bytes or characters. <p>Domain – Choose a domain. A domain is a named combination of built-in data types, default value, check condition, and nullability.</p> <p>Compress values – Compress column values. If a column is compressed, database server activities such as indexing, data comparisons, and statistics generation may be slightly slower if they involve the compressed column because the values must be compressed when written, and decompressed when read. This option is not available for certain built-in types.</p> <p>Maintain BLOB indexes for large values – Maintain BLOB indexes for large values. Only character, binary, and bit types support this option.</p>

Area	Description
Value	<p>No default or computed value – Select this option if the column is not a computed value and has no default value</p> <p>Default Value – Select this option if the column has a default value. If the column is based on a domain, this setting inherits the domain's default value (if any), but you can override the value for the column. Choosing the Default value option enables the User-defined and System-defined options.</p> <ul style="list-style-type: none"> • User-defined – Type a custom value (string, number, or other expression) for the default value. If you have based the column on a domain, you can retain the domain's default value (if any), or override it for the column • Literal string – Specify whether the default value for the column should be treated as a literal string. By default, this option is selected for character columns and domains with a character base type. You do not need to enclose default text in single quotes, and escape embedded single quotes or backslashes in the string. • System-defined – Lets you select a predefined value (for example, current date) for the default value. Select a value. If you have based the column on a domain, you can retain the domain's default value (if any) or override it for the column. <p>Partition size – When you select global autoincrement, the domain of values for that column is partitioned. Each partition contains the same number of values. For example, if you set the partition size for an integer column in a database to 1000, one partition extends from 1001 to 2000, the next from 2001 to 3000, and so on.</p> <p>Computed Value – Define a computed value for the column. A computed column derives its values from calculations of values in other columns. Type an expression in the text box to describe the relationship between the other columns and the value that appears in the computed column.</p>
Constraints	<p>Values can be null – Select this option if null values are allowed in the column. If the column is based on a domain, you can retain the domain's nullability or override it for the column.</p> <p>Values cannot be null – Select this option to allow duplicate values, but not allow null values in this column.</p> <p>Values cannot be null and must be unique – Select this option if values in the column cannot be null and must be unique.</p>

Area	Description
Placement	Select the placement details for this column – (For non-global tables within the IQ main store) Select a dbspace. The database server places the column in the selected dbspace. Only those dbspaces in read-write mode, and those dbspaces for which the user has permissions, appear in the list.

7. Click **OK** to close the Column Properties view.
8. Do one of the following:
 - Click **Edit** to modify additional columns in the table.
 - Click **Apply** to update any column changes to the Table Properties view and remain in the Column Properties view.
 - Click **OK** to update any column changes to the Table Properties view and exit the Column Properties view.

Clicking **OK** or **Apply** in the Column Properties view updates any changes to the Table Properties dialog. It does NOT save the changes to the database.

9. Click **OK** to save any changes in the Table Properties view to the database.

See also

- *Adding a Column* on page 529
- *Deleting a Column* on page 533
- *Table Column Privilege Summary* on page 540
- *Authenticating a Login Account for a Managed Resource* on page 282

Table Column Privilege Summary

A list of the system privileges and object permissions required to complete the various table column tasks.

Adding a Column

Database Version	Table Column Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Create a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER permission on the table. • You own the underlying table. <p>Create a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER and REFERENCE permission on the table. • You own the underlying table.
SAP Sybase IQ 16.0	<p>Create a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of the following: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the underlying table. <p>Create a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of the following: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • Both ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

Deleting a Column

Database Version	Table Column Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Deleting a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER permission on the table. • You own the underlying table. <p>Deleting a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER and REFERENCE permission on the table. • You own the underlying table.
SAP Sybase IQ 16.0	<p>Deleting a column without a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the underlying table. • You own the underlying table. <p>Deleting a column with a primary key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • Both ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

Viewing or Modify Column Properties

Database Version	Table Column Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any table column property page – None required.</p> <p>Modify the Primary key property on the General page – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Both ALTER and REFERENCE permission on the table. • You own the table. <p>Modify any other table column property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • You own the table.
SAP Sybase IQ 16.0	<p>View any table column property page – None required.</p> <p>Modify the Primary key property on the General page – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • Both ALTER and REFERENCE permission on the table. • You own the table. <p>Modify a table column comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>Modify any other table column property – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table. • You own the table.

See also

- *Adding a Column* on page 529

- *Deleting a Column* on page 533
- *Viewing or Modifying Column Properties* on page 535

Table Permissions

Grant or revoke table permissions to users and roles.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617

About the Tables Permissions List

The Tables permissions list displays details on the specific object permissions directly granted to users or roles for a single view.

There are several table object permissions, which can be granted with or without administrative rights. Some permissions can be granted at table level only, while others can be granted at either the table or column level.

- SELECT – table or column level

- INSERT – table level only
- DELETE – table level only
- UPDATE – table or column level
- ALTER – table level only
- REFERENCE – table or column level
- LOAD – table level only
- TRUNCATE – table level only

These object permissions can be granted in several ways:

- You own the object.
- You are granted the **MANAGE ANY OBJECT PRIVILEGE** system privilege.
- You have been indirectly granted specific permissions through membership in a role to which permissions have been directly or indirectly granted.
- You have been directly granted specific permissions.

Users or roles with object ownership or the **MANAGE ANY OBJECT PRIVILEGE** system privilege are automatically granted all possible object permissions with administrative rights.

Object permissions can be granted with or without administrative rights. When granted without administrative rights, the grantee can perform authorized tasks requiring the permission, but cannot in turn grant the permission to another user or role. When granted with administrative rights (With grant option), the grantee can do both.

The permissions list only lists those permissions granted directly to user or roles. The list indicates which columns the permissions are granted to, to whom (grantee), by who (grantor), and the permissions and their corresponding administrative rights. The permissions list does not list object permissions obtained through ownership, the **MANAGE ANY SYSTEM OBJECT** system privilege, or role membership.

The permissions list only lists those permissions granted directly to user or roles. The list indicates which columns the permissions are granted to, to whom (grantee), by who (grantor), and the permissions and their corresponding administrative rights. The permissions list does not list object permissions obtained through ownership, the **MANAGE ANY SYSTEM OBJECT** system privilege, or role membership.

Permissions granted to all columns on the table are listed first. The remainder of the list is sorted alphabetically, by column name.

Permissions										
Column	Grantee	grantor	Select	Insert	Delete	Update	Alter	Referenc	Load	Truncate
All	Jane	Bob		✓		✓		✓		
All	Manager	Manager	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔
aaa	Alice	Alex	✓ ↔					✓ ↔		
bbb	Alice	Alex	✓ ↔					✓ ↔		
<div>Legend: ✓ Permission granted with no administrative rights ✓ ↔ Permission granted with administrative rights</div>										

When granted to a role, permissions, including administrative rights, are inherited by all members of the role. The role, not the users indirectly granted the permissions through inheritance, appear on the permissions list.

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the SELECT permission with the With grant option. UserA grants SELECT to UserB with the With grant option. UserB grants SELECT to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the SELECT permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

Permissions can be granted on the same column, to the same grantee, by multiple grantors, resulting in the same grantee appearing multiple times on the list. If the same permission is granted to the same grantee, with and without administrative rights, the grant with the administrative right takes precedence.

Column	Grantee	grantor	Select	Insert	Delete	Update	Alter	Referenc	Load	Truncate
All	Jane	Bob		✓		✓		✓		
All	Manager	Manager	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔
aaa	Alice	Alex	✓ ↔					✓ ↔		
aaa	Alice	Bob	✓							
bbb	Alice	Alex	✓ ↔					✓ ↔		
ccc	Jane	Alex						✓ ↔		

In this example, Jane is granted permissions by both Bob and Alex. Bob grants Jane permissions on all columns, while Alex only grants permissions on column ccc. Jane has INSERT, UPDATE, and REFERENCE permissions without administrative rights on all columns in the table (granted by Bob). However, she also has REFERENCE permission on column ccc only (granted by Alex). When the same permission is granted with different administrative rights the higher administrative right takes precedence, at the specific level.

Therefore, the REFERENCE permission with administrative rights only applies to column ccc on the table.

When revoking a permission granted multiple times, the permission is revoked from all instances, regardless of administrative rights. For example, Manager1 grants User2 INSERT with administrative rights. User1 also grants INSERT to User2, but without administrative rights. Regardless of which instance of INSERT is revoked, both instances of INSERT are revoked for User2.

Following the Table Permissions Grant Trail

Before revoking a grantee's permission, you need to identify grantees directly or indirectly granted the permission from the original grantee.

The grant chain traces how a grantee has in turn granted a permission to other grantees.

Consider the following:

- Bob is granted all permissions with administrative rights to all columns in the table.
- Bob grants Joe SELECT permission without administrative rights to column bbb only. Bob also grants Jane SELECT and INSERT permissions with administrative rights to all columns.
- Jane grants Mike and Joe SELECT and REFERENCE permissions with administrative rights to columns aaa and bbb. Jane also grants Beth and Mary UPDATE permissions without administrative rights on column ccc.

Note: Joe has now been granted the SELECT permission twice, with different administrative rights, by different grantors, to different columns.

- Joe grants Beth UPDATE permission without administrative rights to all columns in the table.

Note: Beth has now been granted the UPDATE permission twice, by different grantors, at both the column and table level.

- Mike grants Sarah ALTER permission with administrative rights to all columns in the table. Mike also grants Alice ALTER permission without administrative rights, again to the whole table.
- Sarah grants Alex and Beth ALTER and UPDATE permissions without administrative rights on all columns.

Note: Beth has now been granted the ALTER permission multiple times, by different grantors, on different columns.

The permissions list would appear similar to:

You want to revoke SELECT permission from Jane. To determine the potential impact on other users and roles, do the following:

Tip: For complex grant trails, create a tree diagram to visually track the grant chain.

- Sort the list by Grantor and locate all instances of administrative grants of SELECT by Jane.

Column	Grante	grantor 1 ▲	Select	Insert	Delete	Update	Alter	Refere	Load	Trunca
All	Jane	Bob	✓ ↔	✓ ↔						
bbb	Joe	Bob	✓							
aaa	Mike	Jane	✓ ↔					✓ ↔		
aaa	Joe	Jane	✓ ↔					✓ ↔		
bbb	Mike	Jane	✓ ↔					✓ ↔		
bbb	Joe	Jane	✓ ↔					✓ ↔		
All	Beth	Joe				✓				
All	Bob	Manager	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔
All	Alice	Mike					✓			
All	Sarah	Mike					✓ ↔			
All	Alex	Sarah				✓	✓			
All	Beth	Sarah				✓	✓			

Note: There are four instances of Jane granting permissions. Since we are revoking the SELECT permission only, only those grants involving the SELECT permission will be impacted. Therefore, revoking Jane's SELECT permission will also revoke the permission from Mike and Joe, on columns aaa and bbb. Of the SELECT permissions, you only need to follow those involving administrative rights.

- Locate Mike in the Grantor column.

Column	Grante	grantor 1 ▲	Select	Insert	Delete	Update	Alter	Refere	Load	Trunca
All	Jane	Bob	✓ ↔	✓ ↔						
bbb	Joe	Bob	✓							
aaa	Mike	Jane	✓ ↔					✓ ↔		
aaa	Joe	Jane	✓ ↔					✓ ↔		
bbb	Mike	Jane	✓ ↔					✓ ↔		
bbb	Joe	Jane	✓ ↔					✓ ↔		
All	Beth	Joe				✓				
All	Bob	Manager	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔
All	Alice	Mike					✓			
All	Sarah	Mike					✓ ↔			
All	Alex	Sarah				✓	✓			
All	Beth	Sarah				✓	✓			

Note: Mike granted ALTER to Sarah and Alice. Both were granted the SELECT permission as an indirect (once removed) result of Jane. It does not matter whether the grant included administrative rights. Therefore, their SELECT permission will also be revoked when Jane's is revoked. Since Alice was granted SELECT without administrative

rights, her grant chain ends. Since Sarah was granted SELECT with administrative rights, her grant chain continues.

3. Locate Sarah in the Grantor column.

Column	Grantee	grantor 1 ▲	Select	Insert	Delete	Update	Alter	Refere	Load	Trunca
All	Jane	Bob	✓ ↔	✓ ↔						
bbb	Joe	Bob	✓							
aaa	Mike	Jane	✓ ↔					✓ ↔		
aaa	Joe	Jane	✓ ↔					✓ ↔		
bbb	Mike	Jane	✓ ↔					✓ ↔		
bbb	Joe	Jane	✓ ↔					✓ ↔		
All	Beth	Joe				✓				
All	Bob	Manager	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔
All	Alice	Mike					✓			
All	Sarah	Mike					✓ ↔			
All	Alex	Sarah				✓	✓			
All	Beth	Sarah				✓	✓			

Note: Sarah granted ALTER and UPDATE to Beth and Alex. Both were granted the SELECT permission as an indirect (twice removed) result of Jane. Again, administrative rights do not matter, and since neither grant was with administrative rights, the grant chain ends.

To summarize, revoking Jane's SELECT permission revokes the permission from Mike, Joe, Beth, and Mary, through direct granting or permissions by Jane, but also revokes the permission from Alice, Sarah, Alex, and Role1 as a result of indirect from Jane. The permissions list after revoking Jane's SELECT permission would appear similar to:

Column	Grantee	grantor 1 ▲	Select	Insert	Delete	Update	Alter	Refere	Load	Trunca
All	Jane	Bob	✓ ↔	✓ ↔						
bbb	Joe	Bob	✓							
aaa	Mike	Jane	✓ ↔					✓ ↔		
aaa	Joe	Jane	✓ ↔					✓ ↔		
bbb	Mike	Jane	✓ ↔					✓ ↔		
bbb	Joe	Jane	✓ ↔					✓ ↔		
All	Beth	Joe				✓				
All	Bob	Manager	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔
All	Alice	Mike					✓			
All	Sarah	Mike					✓ ↔			
All	Alex	Sarah				✓	✓			
All	Beth	Sarah				✓	✓			

It is important to note that it is possible for a user to retain an "identified" permission after revoke it the same permission was granted by multiple grantors. In this scenario, both Bob and Jane granted the SELECT permission to Joe, so Joe retains the SELECT permission granted by Bob. If a grantee has been granted multiple permissions, only those permissions explicitly selected are revoked. In this scenario, only the SELECT permission was revoked from Joe. The REFERENCE permission remains granted, even though it was also granted by Jane.

Column	Grantee	grantor 1 ▲	Select	Insert	Delete	Update	Alter	Referen	Load	Truncat
All	Jane	Bob		✓ ↔						
bbb	Joe	Bob	✓							
aaa	Mike	Jane						✓ ↔		
aaa	Joe	Jane						✓ ↔		
bbb	Mike	Jane						✓ ↔		
bbb	Joe	Jane						✓ ↔		
All	Beth	Joe				✓				
All	Bob	Manager	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔
All	Alice	Mike					✓			
All	Sarah	Mike					✓ ↔			
All	Alex	Sarah				✓	✓			
All	Beth	Sarah				✓	✓			

Granting Permissions on a Table

Grant table permissions to users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You have administrative rights (with grant option) to the permission. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, click **Permissions**.
6. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
7. On the Welcome page, indicate whether the permission is being granted to a user or role.
8. Click **Next**.
9. On the Grantees page, select one or more users or roles. Click the box in the header row to select all available users or roles.
10. Click **Next**.
11. On the Columns page, select one or more columns for the selected table to apply the permissions to. Click the box in the header row to select all available columns.
12. Click **Next**.
13. On the Permissions page, select one or more permissions. Click the box in the header row to select all available permissions.
14. (Optional) Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

15. Click **Finish**.
16. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Revoking Permissions on a Table

Remove table permissions from users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You have administrative rights (with grant option) to the permission. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the SELECT permission with the With grant option. UserA grants SELECT to UserB with the With grant option. UserB grants SELECT to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the SELECT permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, click **Permissions**.
6. In the right pane, select a user or role granted permissions to be revoked, and click **Revoke**.
A list of permissions currently granted (regardless of administrative rights) appears..
7. Select one or more permissions to revoke. Click the box in the header row to select all available permissions.

Warning! Revoking permissions may result in unexpected revocation from other users or groups. See *Following the Table Permission Grant Trail*.

8. Click **Finish**.
9. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Removing Administrative Rights Only from a Table Permission

Remove administrative rights only from a granted table permission.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• <code>MANAGE ANY OBJECT PRIVILEGE</code> system privilege.• You have administrative rights to the permission being modified.• You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are logged on as the original grantor of the permission with administrative rights to be removed.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, click **Permissions**.
6. In the right pane, click **Grant**.
7. On the Welcome page, indicate whether the grantee is a user or role.
8. Click **Next**.
9. On the Grantees page, select the grantee.
10. Click **Next**.
11. On the Permissions page, select the permissions from which the administrative rights are being revoked.
12. Click **Finish**.
13. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Adding Administrative Rights to a Granted Table Permission

Add administrative rights only to a granted table permission.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, click **Permissions**.
6. In the right pane, select the grantee to have administrative rights granted on a permission. If the grantee appears on the list multiple times with the same permission granted, it does not matter which instance is selected.
7. In the right pane, click **Grant**.
8. On the Welcome page, indicate whether the grantee is a user or role.
9. Click **Next**.
10. On the Grantees page, select the grantee..

11. Click **Next**.
12. On the Permissions page, select the permissions from which the administrative rights were revoked.
13. Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

14. Click **Finish**.
15. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Manage Permissions on a Proxy Table

The ability to grant object-level permissions at the proxy table level is not implemented in this release of Sybase Control Center. You can, however, grant these permissions at the user or role level.

This means that you cannot grant proxy table permissions to multiple users and roles at the same time. They must be granted one user or role at a time.

Follow the steps under *Role-Based Table and Column Permissions* to grant and revoke proxy table object level permissions. Alternately, at the SQL level, you can execute a **GRANT** object-level permissions statement.

Table Permissions Privilege Summary

A list of the system privileges and object permissions required to complete the various table permission tasks.

Grant and Revoke Permissions on a Table

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You have administrative rights (with grant option) to the permission. • You own the database object.

Database Version	Database Object Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

Adjust Administration Permissions on a Table

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

Table Constraints

Constraints help to ensure that the data entered in the table is correct. Constraints also provide information to SAP Sybase IQ that boosts performance.

SAP Sybase IQ does not allow the creation of a check constraint that it cannot evaluate, such as those composed of user-defined functions, proxy tables, or non-SAP Sybase IQ tables. Constraints that cannot be evaluated are detected the first time the table on which the check constraint is defined is loaded or modified.

Note: SAP Sybase IQ does not allow check constraints containing:

- Subqueries
 - Expressions specifying a host language parameter, a SQL parameter, or a column as the target for a data value
 - Set functions
 - Invocations of nondeterministic functions or functions that modify data
-

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474

- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Indexes* on page 586
- *Table Triggers* on page 606
- *Table Partitions* on page 617

Creating a Column Check Constraint

A column check constraint enforces a specified condition on a column. Add a column check constraint to a table using the Create Constraint Wizard.

Prerequisites

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying table. • You own the underlying table.

Database Version	Table Constraint Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • You have ALTER permission on the underlying table. • You own the underlying table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**, select the table in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. Select **Constraints**.
5. Click **New**.
The Create Constraint Wizard appears.
6. On the Welcome page, specify a column check constraint:

Option	Description
Select the type of constraint	From the Select an item pull-down, select Column check constraint.

7. Click **Next**.
8. On the Constraint Name page, specify:

Option	Description
What do you want to name the new column check constraint?	Specify a descriptive name for the column check constraint.
For which column do you want to create the new check constraint?	Filter the Name, Primary Key, Data Type, Size, and Scale columns to locate the desired column. Select a single column you want to create the constraint on.

9. Click **Next**.
10. On the Definition page, specify:

Option	Description
Specify a condition to restrict the values.	SQL definition of the check constraint.

Use this example as a model when specifying a definition:

```
CHECK(TerminationDate >= StartDate);
```

This example adds a constraint on the `Employees` table to ensure that the `TerminationDate` is always later than, or equal to, the `StartDate`.

11. Click **Finish to close the Create Constraint Wizard.**

The Properties view appears.

Tip: Although you closed the Create Constraint Wizard, the constraint is still in-progress until you click **Apply** and **OK** in step 12. If there is a problem with the constraint definition, modify the in-progress constraint by clicking **Properties** and then making the necessary SQL changes.

12. Click **Apply and **OK**.**

See also

- *Creating a Foreign Key Constraint* on page 560
- *Creating a Table Check Constraint* on page 564
- *Creating a Unique Constraint* on page 566
- *Deleting a Table or Column Check Constraint* on page 568
- *Deleting a Primary, Foreign, or Unique Key Constraint* on page 569
- *Rebuilding a Unique, Primary or Foreign Key Constraint* on page 571
- *Validating a Unique, Primary or Foreign Key Constraint* on page 572
- *Generating Constraint DDL Commands* on page 573
- *Viewing or Modifying Constraint Properties* on page 574
- *Table Constraints Privilege Summary* on page 580
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Foreign Key Constraint

A foreign key constraint enforces a restriction on a column specifying how the data in one table relates to the data in another table, or the same table. Add a foreign key constraint to the table using the Create Constraint Wizard.

Prerequisites

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Requires one of: <ul style="list-style-type: none"> • ALTER permission on the derived table • You own the derived table. • Also requires one of: <ul style="list-style-type: none"> • REFERENCE permission on the base table. • You own the base table. • Also requires one of: <ul style="list-style-type: none"> • REFERENCE permission on the derived table (to index it) • You own the derived table.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace the table is defined on, along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the derived table. • You own the derived table. <p>Also requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • REFERENCE permission on the base table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- If you want the foreign key to reference a unique constraint, the unique constraint must exist.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**, select the table in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. Select **Constraints**.
5. Click **New**.
The Create Constraint Wizard appears.
6. On the Welcome page, specify a foreign key constraint:

Option	Description
Select the type of constraint	From the Select an item pull-down, select Foreign key constraint.

7. Click **Next**.
8. On the Table page, select the table you want this foreign key to refer to:

Option	Description
To which table do you want this foreign key to refer?	Filter the Name and Owner columns to locate the desired table. Select a single table you want the foreign key to refer to.
What do you want to name the new foreign key?	Specify a descriptive name for the foreign key.

9. Click **Next**.
10. On the Reference page, specify:

Option	Description
Do you want this foreign key to reference the primary key or a unique constraint?	<ul style="list-style-type: none"> • Primary key – Select this if you want the foreign key to reference the primary key. • Unique constraint – Select this if you want the foreign key to reference an existing unique constraint. Select the unique constraint from the pull-down.

Option	Description
For each primary key column in the referenced table, you must specify the foreign column that it should reference or choose to add a new column to the table.	Filter the Foreign Column, Order, and Primary Key Column to locate the desired column. <ul style="list-style-type: none"> • Foreign Column – Select the foreign column from the pull-down. • Order – Select either Ascending or Descending order from the pull-down.
Add column	(Only displays if no exact match is found for the data type, size, scale, and name of the primary key column) Adds a new primary key column.

11. Click Next.

12. On the Referential Integrity page, specify:

Option	Description
Update action	<ul style="list-style-type: none"> • Not permitted – Generates an error and prevents the modification if an attempt to alter a referenced primary key value occurs. This is the default referential integrity action. • Set values to null – Sets all foreign keys that reference the modified primary key to NULL. • Cascade values – Updates all foreign keys that reference the updated primary key to the new value. • Set values to default – Sets all foreign keys that reference the modified primary key to the default value for that column (as specified in the table definition).
Delete action	<ul style="list-style-type: none"> • Not permitted – Generates an error and prevents the modification if an attempt to alter a referenced primary key value occurs. This is the default referential integrity action. • Set values to null – Sets all foreign keys that reference the modified primary key to NULL. • Cascade values – Deletes all rows containing foreign keys that reference the deleted primary key. • Set values to default – Sets all foreign keys that reference the modified primary key to the default value for that column (as specified in the table definition).
Check only on a commit	Forces the database to wait for a COMMIT before checking the integrity of the foreign key, overriding the setting of the WAIT_FOR_COMMIT database option.

13. Click Next.

14. (System store (IQ catalog store) tables only) On the Clustered Index page, specify:

Option	Description
Create a clustered foreign key	Select if you want to make the constraint's underlying index a clustered index. Clustered indexes can improve performance.

15. Click **Next**.

16. On the Comment page, add an optional, descriptive comment. Comments help you organize your database.

17. Click **Finish** to close the Create Constraint Wizard.
The Properties view appears.

Tip: Although you closed the Create Constraint Wizard, the constraint is still in-progress until you click **Apply** and **OK** in step 18. If there is a problem with the constraint, modify the in-progress constraint by clicking **Properties** and then making the necessary changes.

18. Click **Apply** and **OK**.

See also

- *Creating a Column Check Constraint* on page 557
- *Creating a Table Check Constraint* on page 564
- *Creating a Unique Constraint* on page 566
- *Deleting a Table or Column Check Constraint* on page 568
- *Deleting a Primary, Foreign, or Unique Key Constraint* on page 569
- *Rebuilding a Unique, Primary or Foreign Key Constraint* on page 571
- *Validating a Unique, Primary or Foreign Key Constraint* on page 572
- *Generating Constraint DDL Commands* on page 573
- *Viewing or Modifying Constraint Properties* on page 574
- *Table Constraints Privilege Summary* on page 580
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Table Check Constraint

A table check constraint ensures that no row in a table violates the constraint, which may include more than one column in its specification.

Prerequisites

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • You have ALTER permission on the underlying table. • You own the underlying table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**, select the table in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. Select **Constraints**.
5. Click **New**.
The Create Constraint Wizard appears.
6. On the Welcome page, specify a table check key constraint:

Option	Description
Select the type of constraint	From the Select an item pull-down, select Table check constraint.

7. Click **Next**.
8. On the Constraint Name page, specify:

Option	Description
What do you want to name the new check constraint?	Specify a descriptive name for the check constraint.

9. Click **Next**.

10. On the Definition page, specify:

Option	Description
Specify a condition to restrict the values.	SQL definition of the check constraint.

Use this example as a model when specifying a definition:

```
CHECK(TerminationDate >= StartDate);
```

This example adds a constraint on the `Employees` table to ensure that the *TerminationDate* is always later than, or equal to, the *StartDate*.

Tip: The table check constraint definition can include multiple columns.

11. Click **Next**.

12. On the Comment page, add an optional, descriptive comment. Comments help you organize your database.

13. Click **Finish** to close the Create Constraint Wizard.
The Properties view appears.

Tip: Although you closed the Create Constraint Wizard, the constraint is still in-progress until you click **Apply** and **OK** in step 14. If there is a problem with the constraint, modify the in-progress constraint by clicking **Properties** and then making the necessary changes.

14. Click **Apply** and **OK**.

See also

- *Creating a Column Check Constraint* on page 557
- *Creating a Foreign Key Constraint* on page 560
- *Creating a Unique Constraint* on page 566
- *Deleting a Table or Column Check Constraint* on page 568
- *Deleting a Primary, Foreign, or Unique Key Constraint* on page 569
- *Rebuilding a Unique, Primary or Foreign Key Constraint* on page 571
- *Validating a Unique, Primary or Foreign Key Constraint* on page 572
- *Generating Constraint DDL Commands* on page 573
- *Viewing or Modifying Constraint Properties* on page 574
- *Table Constraints Privilege Summary* on page 580
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Unique Constraint

The unique constraint specifies that one or more columns uniquely identify each row in the table.

Prerequisites

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace the table is defined on, along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

The unique constraint is essentially the same as the primary key constraint, except that you can specify more than one unique constraint in a table. Columns must not contain any NULL values.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**, select the table in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. Select **Constraints**.
5. Click **New**.
The Create Constraint Wizard appears.
6. On the Welcome page, specify a unique constraint:

Option	Description
Select the type of constraint	From the Select an item pull-down, select Unique constraint.

7. Click **Next**.

8. (Optional) On the Constraint Name page, enter a name for the unique constraint, and click **Next**.

If you do not specify a name, the system generates one automatically.

9. On the Columns page, specify:

Option	Description
Add Asc. >>	Moves columns from the Available Columns pane to the Selected Columns pane, in ascending order.
Add Desc. >>	(IQ catalog store (system store) tables only.) Moves columns from the Available Columns pane to the Selected Columns pane, in descending order.
<< Remove	Moves columns from the Selected Columns pane to the Available Columns pane.

10. Click **Next**.

11. (System store (catalog store) tables only) On the clustered index page, specify:

Option	Description
Create a clustered unique constraint	Select if you want to make the constraint's underlying index a clustered index. Clustered indexes can improve performance.

12. Click **Next**.

13. On the Comment page, add an optional, descriptive comment. Comments help you organize your database.

14. Click **Finish** to close the Create Constraint Wizard.

The Properties view appears.

Tip: Although you closed the Create Constraint Wizard, the constraint is still in-progress until you click **Apply** and **OK** in step 15. If there is a problem with the constraint, modify the in-progress constraint by clicking **Properties** and then making the necessary changes.

15. Click **Apply** and **OK**.

See also

- *Creating a Column Check Constraint* on page 557
- *Creating a Foreign Key Constraint* on page 560

- *Creating a Table Check Constraint* on page 564
- *Deleting a Table or Column Check Constraint* on page 568
- *Deleting a Primary, Foreign, or Unique Key Constraint* on page 569
- *Rebuilding a Unique, Primary or Foreign Key Constraint* on page 571
- *Validating a Unique, Primary or Foreign Key Constraint* on page 572
- *Generating Constraint DDL Commands* on page 573
- *Viewing or Modifying Constraint Properties* on page 574
- *Table Constraints Privilege Summary* on page 580
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Table or Column Check Constraint

Delete a table or column check constraint from a table.

Prerequisites

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the underlying table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**, select the table in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. Select **Constraints**.
5. Select one or more table or column check constraints from the list.

Note: Different system privileges are required to delete different constraint types. If you do not have sufficient privilege to delete a selected constraint, the **Delete** button is unavailable.

6. Click **Delete**.
7. The selected constraints are removed from the list, but they are not yet deleted. Click **Apply** and **OK** to complete the deletion process.

See also

- *Creating a Column Check Constraint* on page 557
- *Creating a Foreign Key Constraint* on page 560
- *Creating a Table Check Constraint* on page 564
- *Creating a Unique Constraint* on page 566
- *Deleting a Primary, Foreign, or Unique Key Constraint* on page 569
- *Rebuilding a Unique, Primary or Foreign Key Constraint* on page 571
- *Validating a Unique, Primary or Foreign Key Constraint* on page 572
- *Generating Constraint DDL Commands* on page 573
- *Viewing or Modifying Constraint Properties* on page 574
- *Table Constraints Privilege Summary* on page 580
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Primary, Foreign, or Unique Key Constraint

Delete a primary, foreign, or unique key constraint from a table.

Prerequisites

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**, select the table in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. Select **Constraints**.
5. Select one or more primary, foreign, or unique key constraints from the list.

Note: Different system privileges are required to delete different constraint types. If you do not have sufficient privilege to delete a selected constraint, the **Delete** button is unavailable.

6. Click **Delete**.
7. The selected constraints are removed from the list, but they are not yet deleted. Click **Apply** and **OK** to complete the deletion process.

See also

- *Creating a Column Check Constraint* on page 557
- *Creating a Foreign Key Constraint* on page 560
- *Creating a Table Check Constraint* on page 564
- *Creating a Unique Constraint* on page 566
- *Deleting a Table or Column Check Constraint* on page 568
- *Rebuilding a Unique, Primary or Foreign Key Constraint* on page 571
- *Validating a Unique, Primary or Foreign Key Constraint* on page 572
- *Generating Constraint DDL Commands* on page 573
- *Viewing or Modifying Constraint Properties* on page 574
- *Table Constraints Privilege Summary* on page 580
- *Authenticating a Login Account for a Managed Resource* on page 282

Rebuilding a Unique, Primary or Foreign Key Constraint

Rebuild a unique, primary, or foreign key constraint on a system store (IQ catalog store) table.

Prerequisites

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY INDEX system privilege. • REFERENCE permission on the underlying table. • You own the underlying table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**, select a system store table in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. Select **Constraints**.
5. Select a unique, primary, or foreign key constraint from the list.

Note: Not all constraints can be rebuilt. If a selected constraint cannot be rebuilt, the **Rebuild** button is unavailable.

6. Click **Rebuild**
The Rebuild Constraint view appears indicating the rebuilding status.
7. Click **OK**.

See also

- *Creating a Column Check Constraint* on page 557
- *Creating a Foreign Key Constraint* on page 560

- *Creating a Table Check Constraint* on page 564
- *Creating a Unique Constraint* on page 566
- *Deleting a Table or Column Check Constraint* on page 568
- *Deleting a Primary, Foreign, or Unique Key Constraint* on page 569
- *Validating a Unique, Primary or Foreign Key Constraint* on page 572
- *Generating Constraint DDL Commands* on page 573
- *Viewing or Modifying Constraint Properties* on page 574
- *Table Constraints Privilege Summary* on page 580
- *Authenticating a Login Account for a Managed Resource* on page 282

Validating a Unique, Primary or Foreign Key Constraint

Check the validity of unique, primary, or foreign key constraint on system store (IQ catalog store) table.

Prerequisites

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• VALIDATE authority.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The table is a system store (IQ catalog store) table.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**, select a system store table in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. Select **Constraints**.
5. Select a unique, primary, or foreign key constraint from the list.

Note: Not all constraints can be rebuilt. If a selected constraint cannot be rebuilt, the **Validate** button is unavailable.

6. Click **Validate**.
The Validate Constraint view appears indicating the validation status.

7. Click **OK**.

See also

- *Creating a Column Check Constraint* on page 557
- *Creating a Foreign Key Constraint* on page 560
- *Creating a Table Check Constraint* on page 564
- *Creating a Unique Constraint* on page 566
- *Deleting a Table or Column Check Constraint* on page 568
- *Deleting a Primary, Foreign, or Unique Key Constraint* on page 569
- *Rebuilding a Unique, Primary or Foreign Key Constraint* on page 571
- *Generating Constraint DDL Commands* on page 573
- *Viewing or Modifying Constraint Properties* on page 574
- *Table Constraints Privilege Summary* on page 580
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Constraint DDL Commands

Display the data description language SQL code for adding a constraint to a table. The DDL can be a useful reference and training tool.

Prerequisites

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**, select the table in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. Select **Constraints**.
5. Select a constraint from the list and select **Generate DDL**.

See also

- *Creating a Column Check Constraint* on page 557

- *Creating a Foreign Key Constraint* on page 560
- *Creating a Table Check Constraint* on page 564
- *Creating a Unique Constraint* on page 566
- *Deleting a Table or Column Check Constraint* on page 568
- *Deleting a Primary, Foreign, or Unique Key Constraint* on page 569
- *Rebuilding a Unique, Primary or Foreign Key Constraint* on page 571
- *Validating a Unique, Primary or Foreign Key Constraint* on page 572
- *Viewing or Modifying Constraint Properties* on page 574
- *Table Constraints Privilege Summary* on page 580
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Constraint Properties

View constraint details or change the constraint details and constraint definition of an existing constraint.

Prerequisites

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View table constraint properties – None required.</p> <p>Modify comment on foreign key or unique constraint – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• ALTER permission on the underlying table.• You own the underlying table.

Database Version	Table Constraint Privileges
SAP Sybase IQ 16.0	<p>View any table constraint property page – None required.</p> <p>Modify the comment on a foreign or primary key constraint – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>Modify the comment on a unique key constraint – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • ALTER ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>Modify the definition of a table or column check constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table. <p>Modify any foreign key constraint property on the Action page – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE ANY INDEX system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the table. <p>Modify any other property of a primary, foreign or unique key, table check or column check constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege.

Database Version	Table Constraint Privileges
	<ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the underlying table.

- The SAP Sybase IQ resource is authenticated and running.
- (Modifying properties only) In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**, select the table in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. Select **Constraints**.
5. Select a constraint from the list and click **Edit**.
6. View or modify constraint properties. The properties differ depending on the constraint type.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Column Check Constraint Properties

Area	Description
n/a	Constraint Name – Name of the column check constraint. Constraint Definition – SQL definition of the column check constraint.

Foreign Key Constraint Properties

Area	Description
General	<p>Name – Name of the foreign key constraint.</p> <p>Unique – Shows whether the foreign key is unique.</p> <p>Foreign table – Shows the name of the table the foreign key belongs to, as well as the table's owner.</p> <p>Foreign index – Shows the name of the index used to enforce the foreign key.</p> <p>Primary constraint – Shows the name of the primary key or unique constraint that the foreign key references.</p> <p>Primary constraint type – Shows the type of constraint the foreign key references. This can only be a primary key or a unique constraint.</p> <p>Primary table – The table containing the primary key in the foreign key relationship.</p> <p>Primary index – Shows the name of the index used to maintain the primary key or unique constraint.</p> <p>Comment – Text description of the foreign key constraint. For example, describe the constraint's purpose in the system.</p>

Area	Description
Actions	<p>Allow null values – Determines whether the foreign key columns allow NULL values. To use this option, the foreign key columns must all have Allow Nulls set to Yes.</p> <ul style="list-style-type: none"> • Match type – Shows the match type selected for the foreign key. The match type determines what is considered a match when using a multi-column foreign key where Null values are allowed. This only applies if the foreign key allows Null. <ul style="list-style-type: none"> • Simple – A match occurs for a row in the referencing table if at least one column in the key is NULL, or all the column values match the corresponding column values present in a row of the referenced table. • Full – A match occurs for a row in the referencing table if all column values in the key are NULL, or if all of the column values match the values present in a row of the referenced table. <p>Update Action – Uses one of the following settings to define the behavior of the table when a user tries to update values in the foreign key.</p> <ul style="list-style-type: none"> • Not permitted – Prevents updates of the associated primary table's primary key value if there are no corresponding foreign keys. • Set values to null – Sets all the foreign key values that correspond to the updated primary key of the associated primary table to NULL. To use this option, the foreign key columns must all have Allow null values set to Yes. • Cascade values – Updates the foreign key to match a new value for the associated primary key. • Set values to default – Sets foreign key values that match the updated or deleted primary key value to values specified in the DEFAULT clause of each foreign key column. To use this option, the foreign key columns must all have default values. <p>Delete Action – Uses one of the following settings to define the behavior of the table when a user tries to delete data.</p> <ul style="list-style-type: none"> • Not permitted – Prevents deletion of the associated primary table's primary key value if there are no corresponding foreign keys in the table. • Set values to null – Sets all the foreign key values in the table that correspond to the deleted primary key of the associated primary table to NULL. To use this option, the foreign key columns must all have Allow Nulls set to Yes. • Cascade values – Deletes the rows from the table that match the deleted primary key of the associated primary table. • Set values to default – Sets foreign key values that match the updated or deleted primary key value to values specified in the DEFAULT clause of

Area	Description
	<p>each foreign key column. To use this option, the foreign key columns must all have default values.</p> <p>Check only on a commit – Forces the database to wait for a COMMIT before checking the integrity of the foreign key, overriding the setting of the wait_for_commit database option.</p>
Columns	Column details for columns contained by the foreign key constraint.

Table Check Constraint Properties

Area	Description
n/a	<p>Constraint Name – Name of the column check constraint.</p> <p>Type – (read-only) Identifies the constraint as a table check constraint.</p> <p>Table – (read-only) Table name.</p> <p>Constraint Definition – SQL definition of the table check constraint.</p>

Unique Constraint Properties

Area	Description
General	<p>Name – Unique constraint name.</p> <p>Index – (read only) Index name.</p> <p>Comment – Text description of the unique constraint. For example, describe the constraint's purpose in the system.</p>
Columns	Column details for the column contained by the unique constraint.

Primary Key Constraint Properties

Area	Description
General	<p>Name – Primary key name.</p> <p>Index – (read only) Index name.</p> <p>Comment – Text description of the primary key constraint. For example, describe the constraint's purpose in the system.</p>
Columns	Column details for the column contained by the primary key constraint.

7. Click **OK.**

The Properties view appears.

Tip: If you modified any properties, the constraint is still in-progress until you click **Apply** and **OK** in step 8. If there is a problem with the constraint, modify the in-progress constraint by clicking **Properties** and then making the necessary changes.

8. Click **Apply and **OK**.****See also**

- *Creating a Column Check Constraint* on page 557
- *Creating a Foreign Key Constraint* on page 560
- *Creating a Table Check Constraint* on page 564
- *Creating a Unique Constraint* on page 566
- *Deleting a Table or Column Check Constraint* on page 568
- *Deleting a Primary, Foreign, or Unique Key Constraint* on page 569
- *Rebuilding a Unique, Primary or Foreign Key Constraint* on page 571
- *Validating a Unique, Primary or Foreign Key Constraint* on page 572
- *Generating Constraint DDL Commands* on page 573
- *Table Constraints Privilege Summary* on page 580
- *Authenticating a Login Account for a Managed Resource* on page 282

Table Constraints Privilege Summary

A list of the system privileges and object permissions required to complete the various table constraints tasks.

Creating a Column Check Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • You have ALTER permission on the underlying table. • You own the underlying table.

Creating a Foreign Key Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • Requires one of: <ul style="list-style-type: none"> • ALTER permission on the derived table • You own the derived table. • Also requires one of: <ul style="list-style-type: none"> • REFERENCE permission on the base table. • You own the base table. • Also requires one of: <ul style="list-style-type: none"> • REFERENCE permission on the derived table (to index it) • You own the derived table.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace the table is defined on, along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the derived table. • You own the derived table. <p>Also requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • REFERENCE permission on the base table.

Creating a Table Check Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying table. • You own the underlying table.

Database Version	Table Constraint Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • You have ALTER permission on the underlying table. • You own the underlying table.

Creating a Unique Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace the table is defined on, along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

Deleting a Table or Column Check Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the underlying table.

Deleting a Unique, Primary or Foreign Key Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER and REFERENCE permission on the underlying table. • You own the underlying table.

Rebuilding a Unique, Primary or Foreign Key Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table. • You own the underlying table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY INDEX system privilege. • REFERENCE permission on the underlying table. • You own the underlying table.

Validating a Constraint

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • VALIDATE authority.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

Generating Constraint DDL Commands

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Constraint Properties

Database Version	Table Constraint Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View table constraint properties – None required.</p> <p>Modify comment on foreign key or unique constraint – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying table. • You own the underlying table.

Database Version	Table Constraint Privileges
SAP Sybase IQ 16.0	<p>View any table constraint property page – None required.</p> <p>Modify the comment on a foreign or primary key constraint – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>Modify the comment on a unique key constraint – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • ALTER ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the table. <p>Modify the definition of a table or column check constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table. <p>Modify any foreign key constraint property on the Action page – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE ANY INDEX system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the table. <p>Modify any other property of a primary, foreign or unique key, table check or column check constraint – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege.

Database Version	Table Constraint Privileges
	<ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table. • You own the underlying table.

See also

- *Creating a Column Check Constraint* on page 557
- *Creating a Foreign Key Constraint* on page 560
- *Creating a Table Check Constraint* on page 564
- *Creating a Unique Constraint* on page 566
- *Deleting a Table or Column Check Constraint* on page 568
- *Deleting a Primary, Foreign, or Unique Key Constraint* on page 569
- *Rebuilding a Unique, Primary or Foreign Key Constraint* on page 571
- *Validating a Unique, Primary or Foreign Key Constraint* on page 572
- *Generating Constraint DDL Commands* on page 573
- *Viewing or Modifying Constraint Properties* on page 574

Table Indexes

You can add multiple indexes to any column in a table to better support the queries you plan to run.

It is more efficient to create all the indexes needed before you insert any data into your database. You can drop any of the optional indexes later if you decide you do not need them.

Indexes can greatly improve the performance of searches on the indexed columns. However, indexes take up space within the database and slow down insert, update, and delete operations. This section helps you determine when you should create an index and how to achieve maximum performance from your index.

There are many situations in which creating an index improves the performance of a database. An index provides an ordering of a table's rows based on the values in some or all of the columns. An index allows the database server to find rows quickly. It permits greater concurrency by limiting the number of database pages accessed. An index also affords the database server a convenient means of enforcing a uniqueness constraint on the rows in a table.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481

- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Triggers* on page 606
- *Table Partitions* on page 617

Column Index Types

Each type of column index is designed to speed processing of a certain kind of data.

These index types are unique to column-based IQ data and cannot be applied to tables in the catalog store.

SAP Sybase IQ assumes you add either an LF or HG index to every column mentioned in a WHERE clause and in a GROUP BY clause.

When you designate a column or set of columns as either a PRIMARY KEY or UNIQUE, the database server automatically creates a High_Group index for it. Choose one PRIMARY KEY from all UNIQUE constraints for the table. Neither PRIMARY KEY nor UNIQUE constraints allow nulls; however, a unique index does allow them. UNIQUE constraints also provide hints on column constraints to the query optimizer.

The database server always uses the fastest index available for the current query or join predicate. If you have not created the index types the query optimizer would ideally use for a column, the server can still resolve queries involving the column, but response time may be slower than it would be with the correct index type or types.

Table 45. Index Types

Index Type	Purpose
Compare (CMP)	Stores the binary comparison (<, >, =, <=, >=, or NE) of any two columns with identical data types, precision, and scale.
DATE	An index on columns of data type DATE used to process queries involving date quantities.
Datetime (DTTM)	An index on columns of data type DATETIME or TIMESTAMP used to process queries involving datetime quantities.
High_Group (HG)	An enhanced B-tree index to process equality and group by operations on high-cardinality data. Recommended only for more than 1,000 distinct values or for a table with less than 25,000 rows.
High_Non_Group (HNG)	A nonvalue-based bitmap index ideal for most high-cardinality DSS operations involving ranges or aggregates.
Low_Fast (LF)	A value-based bitmap index for processing queries on low-cardinality data. Recommended only for up to 1,000 distinct values and more than 25,000 rows in the table. Can support up to 10,000 distinct values.
TIME	An index on columns of data type TIME used to process queries involving time quantities.
WD	Used to index keywords by treating the contents of a CHAR, VARCHAR, or LONG VARCHAR column as a delimited list.
Text	Used to index terms (words) and their positions. Provides ability to search for individual terms, phrases, pairs of terms within specified distances and given order, as well as combinations of these conditions.

Creating an Index on an IQ System Store Table

Create an index on an IQ system store (catalog store) table.

Prerequisites

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires CREATE permission on the specified dbspace.</p> <p>Also requires one of:</p> <ul style="list-style-type: none"> • DBA authority • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	<p>Requires CREATE permission on the specified dbspace.</p> <p>Also requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected table is a base or global temporary table.

Task

Indexes improve search performance on the indexed column or columns. Indexes take up space in the database, however, and slow down the performance of insert, delete, and update operations.

When creating indexes, the order in which you specify the columns becomes the order in which the columns appear in the index. Duplicate references to column names in the index definition are not allowed.

1. Navigate to the Tables Properties page of an IQ system store (catalog store) table.
2. In the left pane, select **Indexes**.

Note: **Indexes** does not appear for Proxy tables as they are not supported.

3. Click **New**.
4. On the Index Name page, specify a name for the index.
5. Click **Next**.

6. On the Columns page, highlight one or more columns and click **Add Asc** or **Add Desc**

Note: Use **Shift-click** or **Control-click** to select multiple columns.

- a) In the **Columns in index** list, highlight a single column and click the up and down buttons to reposition the column.
 - b) Highlight one or more columns and click **Remove** to remove columns from the index.
7. Click **Next**.
8. On the Uniqueness page, indicate if the index is unique.
9. Click **Next**.
10. On the Index Clustering page, indicate if the index is clustered and the dbspace to store the index.
11. Click **Next**.
12. (Optional) On the Comment page, enter a text comment for the index.
13. Click **Finish**.
The index appears in the properties view, but is not saved to the database.
14. Do one of the following:
 - Click **Apply** to upload any property changes to the database and remain in the properties view.
 - Click **OK** to upload any property changes to the database and exit the properties view.
 - Click **Cancel** to cancel any unsaved property changes and exit the properties view.

See also

- *Column Index Types* on page 587
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating an Index on an IQ Store Table

Create an index on an IQ store (main store) table.

Prerequisites

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires CREATE permission on the specified dbspace. Also requires one of: <ul style="list-style-type: none"> • DBA authority • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

Database Version	Table Index Privileges
SAP Sybase IQ 16.0	<p>Requires CREATE permission on the specified dbspace.</p> <p>Also requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected table is a base or global temporary table.

Task

Indexes improve search performance on the indexed column or columns. Indexes take up space in the database, however, and slow down the performance of insert, delete, and update operations.

When creating indexes, the order in which you specify the columns becomes the order in which the columns appear in the index. Duplicate references to column names in the index definition are not allowed.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, select **Indexes**.

Note: **Indexes** does not appear for Proxy tables as they are not supported.

6. Click **New**.
7. On the Index Name page, specify a name for the index.
8. Click **Next**.
9. On the Index Type page, select the type of index.

10. Enter a value in the notify count field if you want to be notified after a specified number of inserts to the index. Default value is 100000. To disable notification, enter zero (0) in the field.
11. Click **Next**.
12. (For index type Word only) (Optional) Enter a word separator character and a maximum word length permitted in the index. Default value is 255 characters.
13. Click **Next**.
14. On the Dbspace page, indicate if the index is to be unique and the dbspace in which to store the index.
15. Click **Next**.
16. On the Columns page, highlight one or more columns and click **Add Asc** or **Add Desc**

Note: Use **Shift-click** or **Control-click** to select multiple columns.

 - a) In the **Columns in index** list, highlight a single column and click the up and down buttons to reposition the column.
 - b) Highlight one or more columns and click **Remove** to remove columns from the index.
17. Click **Next**.
18. (Optional) On the Comment page, enter a text comment for the index.
19. Click **Finish**.

The index appears in the properties view, but is not saved to the database.
20. Do one of the following:
 - Click **Apply** to upload any property changes to the database and remain in the properties view.
 - Click **OK** to upload any property changes to the database and exit the properties view.
 - Click **Cancel** to cancel any unsaved property changes and exit the properties view.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Table Index

Unused indexes take up space in your database. Delete a table index if you do not require it.

Prerequisites

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY INDEX system privilege. • DROP ANY OBJECT system privilege. • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, select **Indexes**.

Note: **Indexes** does not appear for Proxy tables as they are not supported.

6. Select one or more indexes from the right pane.

Note: Use **Shift-click** or **Control-click** to select multiple indexes.

7. Click **Delete**.

Warning! There is no confirmation prompt before the indexes are deleted

8. Do one of the following:

- Click **Apply** to upload any property changes to the database and remain in the properties view.
- Click **OK** to upload any property changes to the database and exit the properties view.
- Click **Cancel** to cancel any unsaved property changes and exit the properties view.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Rebuilding a Table Index

As data is modified in the underlying tables that the indexes operate on, the indexes become fragmented. Rebuild fragmented indexes on tables to improve performance.

Prerequisites

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• RESOURCE authority with REFERENCE permission on the underlying table of the index.• You own the underlying table of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• ALTER ANY INDEX system privilege.• ALTER ANY OBJECT system privilege.• REFERENCE permission on the underlying table of the index.• You own the underlying table of the index.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, select **Indexes**.

Note: **Indexes** does not appear for Proxy tables as they are not supported.

6. Select one or more indexes from the right pane and click **Rebuild**.

Note: Use **Shift-click** or **Control-click** to select multiple indexes.

The Rebuild Indexes view appears when complete and indicates the rebuild status of each selected index.

7. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Validating a Table Index

Validate an index on an IQ system store (catalog store) table. You cannot validate indexes on tables in the IQ store (main store).

Prerequisites

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	Require VALIDATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The table is an IQ system store (catalog store) table.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Tables**.

3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, select **Indexes**.

Note: **Indexes** does not appear for Proxy tables as they are not supported.

6. Select one or more indexes from the right pane and click **Validate**.

Note: Use **Shift-click** or **Control-click** to select multiple indexes.

Note: **Validate** does not appear when the underlying table is an IQ store (main store) table.

The Validate Indexes view appears when complete and indicates the validation status of each selected index.

7. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Moving a Table Index

Move an index from the current dbspace to another dbspace. This action is only applicable to tables in the IQ store (main store).

Prerequisites

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• SPACE ADMIN authority.• CREATE permission on the target dbspace, along with one of:<ul style="list-style-type: none">• You own the underlying table.• You have REFERENCE permission on the underlying table.

Database Version	Table Index Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • You own the underlying table of the index. • Reference permission on the table along with one of: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the target dbspace.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The table is an IQ store (main store) table.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, select **Indexes**.

Note: **Indexes** does not appear for Proxy tables as they are not supported.

6. Select an index from the right pane and click **Move**.

Note: **Move** does not appear when the underlying table is an IQ system store table.

7. In the Move Objects Dialog view, select the new dbspace and click **OK**.
The index is moved, but is not saved to the database.
8. Do one of the following:
 - Click **Apply** to upload any property changes to the database and remain in the properties view.
 - Click **OK** to upload any property changes to the database and exit the properties view.
 - Click **Cancel** to cancel ALL unuploaded property changes and exit the properties view.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Table Index DDL Commands

Display the data description language SQL code for adding an index to a table. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.
4. Select a table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, select **Indexes**.

Note: **Indexes** does not appear for Proxy tables as they are not supported.

6. Select one or more indexes from the right pane and click **Generate DDL**.

Note: Use **Shift-click** or **Control-click** to select multiple indexes.

7. Click **Generate DDL**.

The DDL window shows the SQL code used to add the selected index to the table or materialized view.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Table Index Properties

Display and edit the properties for the selected table index.

Prerequisites

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View table index fragmentation property page – Requires EXECUTE permission on the sp_iqindexfragmentation system procedure to display content of page.</p> <p>View any other table index property page – None required.</p> <p>Modify any index property – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• RESOURCE authority with REFERENCE permission on the underlying table of the index.• You own the underlying table of the index.

Database Version	Table Index Privileges
SAP Sybase IQ 16.0	<p>View table index fragmentation property page –</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sp_iqindexfragmentation system procedure to display content of page. • If the system procedure security model* of the selected database is set to Invoker, you require the MANAGE ANY DBSPACE system privilege to display content of page. <p>*The system procedure security model of the selected database appears on the General page of database properties.</p> <p>View any other table index property page – None required.</p> <p>Modify a table index comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • ALTER ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the underlying table of the index. <hr/> <p>Note: ALTER permission on the table is not required to modify the comment only.</p> <hr/> <p>Modify any other table index property –</p> <ul style="list-style-type: none"> • Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY INDEX system privilege, • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

- The SAP Sybase IQ resource is authenticated and running.
- (Modifying properties only) In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Global Temporary Tables**.

4. Select a table from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The Table Properties view appears.

5. In the left pane, select **Indexes**.

Note: **Indexes** does not appear for Proxy tables as they are not supported.

6. Click **Edit**.

The Indexes Properties view appears.

7. View or modify the properties.

- Any modifications to the properties are saved when either **Apply** or **OK** is clicked
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – Name of the index.</p> <p>Unique – (Read-only) Whether values in the index must be unique. The unique value is set when you create a new index.</p> <p>Table – (Read-only) Name and owner of the table with which the index is associated.</p> <p>DbSPACE – (Read-only) Database file, or dbSPACE, where the index is located.</p> <p>Index Type – (Read-only) (IQ store (main store) tables only) Index type (High Non-Group, for example).</p> <p>Clustered – (Read-only) (IQ system store (catalog store) tables only) Whether this is a clustered index. Clustered indexes store the table rows in approximately the same order as they appear in the corresponding index. Using a clustered index can lead to performance benefits by reducing the number of times each page needs to be read into memory. Only one index on a table can be a clustered index.</p> <p>Format – (Read-only) (IQ system store tables only) The store type of the index.</p> <p>Comment – User-defined text description of the index. For example, the index's purpose in the system.</p>

Area	Description
Columns (Read-only)	<p>Name – Name of the columns indexed.</p> <p>Sequence – Columns are sorted by their sequence, which is a unique number starting at 0. The order of the numbers determines the relative position of the columns in the index.</p> <p>Order – Either ascending or descending order. Set the order when you create a new index.</p> <p>Data Type – Data type of the columns indexed.</p>
Placement (Read-only) (IQ store tables only)	<p>Dbospace – Dbspace occupied by the object.</p> <p>Size – Size of the object.</p> <p>% File – Percentage of the file used by this object.</p> <p>First Block – First block used by this object.</p> <p>Last Block – Last block used by this object.</p>
Fragmentation (Read-only) (IQ store tables only)	<p>Fill Percent – Range of how full pages are, for example, between 11 and 20% full. All percentages are truncated to the nearest percentage point.</p> <p>BTree Pages – Number of B-tree pages in the index with a particular fill percent.</p> <p>GArray Pages – Number of GArray pages in the index with a particular fill percent.</p> <p>Bitmap Pages – Number of bitmap pages in the index with a particular fill percent.</p>

8. Click **OK**.

Index property modifications are not yet saved to the database.

9. Do one of the following:

- Click **Apply** to upload any property changes to the database and remain in the properties view.
- Click **OK** to upload any property changes to the database and exit the properties view.
- Click **Cancel** to cancel ALL unuploaded property changes and exit the properties view.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Table Index Privilege Summary

A list of the system privileges and object permissions required to complete the various index tasks on tables.

Creating a Table Index

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires CREATE permission on the specified dbspace. Also requires one of: <ul style="list-style-type: none"> • DBA authority • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	Requires CREATE permission on the specified dbspace. Also requires one of: <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

Deleting a Table Index

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY INDEX system privilege. • DROP ANY OBJECT system privilege. • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

Rebuilding a Table Index

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

Validating a Table Index

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the underlying table of the index. • You own the underlying table of the index.
SAP Sybase IQ 16.0	Require VALIDATE ANY OBJECT system privilege.

Moving a Table Index

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority. • CREATE permission on the target dbspace, along with one of: <ul style="list-style-type: none"> • You own the underlying table. • You have REFERENCE permission on the underlying table.

Database Version	Table Index Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • You own the underlying table of the index. • Reference permission on the table along with one of: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the target dbspace.

Generating Index DDL Commands

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Index Properties

Database Version	Table Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View table index fragmentation property page – Requires EXECUTE permission on the sp_iqindexfragmentation system procedure to display content of page.</p> <p>View any other table index property page – None required.</p> <p>Modify any index property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

Database Version	Table Index Privileges
SAP Sybase IQ 16.0	<p>View table index fragmentation property page –</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sp_indexfragmentation system procedure to display content of page. • If the system procedure security model* of the selected database is set to Invoker, you require the MANAGE ANY DBSPACE system privilege to display content of page. <p>*The system procedure security model of the selected database appears on the General page of database properties.</p> <p>View any other table index property page – None required.</p> <p>Modify a table index comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • ALTER ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the underlying table of the index. <hr/> <p>Note: ALTER permission on the table is not required to modify the comment only.</p> <hr/> <p>Modify any other table index property –</p> <ul style="list-style-type: none"> • Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY INDEX system privilege, • REFERENCE permission on the underlying table of the index. • You own the underlying table of the index.

Table Triggers

A trigger is a special form of stored procedure that executes automatically when a statement that modifies data in a table is executed. Trigger management includes creating, modifying and deleting triggers on a database object.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479

- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Partitions* on page 617

Creating a Table Trigger

Create a new trigger on a table in the system store.

Prerequisites

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority, along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.

Database Version	Table Trigger Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege. • CREATE ANY OBJECT system privilege. <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The table on which the trigger resides is a system store (catalog store) table.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Proxy Tables**.
4. Select a table or proxy table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table or Proxy Table Properties view appears.

5. In the left pane, select **Triggers**.

Note: **Triggers** does not appear when the selected table is not a system store table.

6. In the right pane, click **New**.
The Create Trigger Wizard appears.
7. On the Welcome page, enter a unique name for the new trigger.
8. Click **Next**.
9. On the Events page, select one or more events to cause the trigger to fire.

Note: When **Update with Columns** is selected, all other events become disabled.

- a) (Update with Columns only) Select one or more columns which cause the trigger to fire when updated.

10. Click **Next**.

11. On the Level page, indicate whether the trigger is to fire at the row or statement level.
12. Click **Next**.
13. On the Timing page, specify:

Option	Description
When do you want the trigger to be fired?	<p>Specify when the trigger is to fire. Availability of timing options is determined by events and levels specified.</p> <ul style="list-style-type: none"> • Before the event – Option disabled when Level = Statement-level • Instead of the event – Option disabled when Event = Update of Columns. • After the event • On a SQL Remote conflict – Option available when Level = Row-level or Event = Update of Columns only
What order in the firing list do you want for this trigger?	<p>Assign a firing order to the trigger to ensure that triggers of the same type that fire at the same time fire in a specific order.</p> <hr/> <p>Note: This option is unavailable when Instead of the event is selected.</p> <hr/>

14. Click **Next**.
15. On the SQL page, enter the statement to be executed when the trigger fires. Triggers do not fire after the execution of **LOAD TABLE**, **TRUNCATE**, or **WRITETEXT** statements.
 The statement window provides a template on which to build the trigger statement. The parameters displayed are based on the options selected in the preceding pages. Once you have made any changes in the statement window, if you return to any of the preceding pages and change any option, when you return to the **SQL** page, the contents of the statement window is overwritten with the base template; any customizations are lost.
16. Click **Next**.
17. On the Comment page, enter an optional comment.
18. Click **Finish**.

Note: Unlike other wizards launched from the properties view, changes to triggers take effect immediately. You do not need to click **OK** or **Apply** in the properties view to upload the change to the database.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Table Trigger

Delete triggers from a table.

Prerequisites

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority, along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • You own the underlying table of the trigger.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. Navigate to the Tables Properties page.
2. In the left pane, select **Triggers**.

Note: **Triggers** does not appear when the selected table is not a system store table.

3. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
4. In the left pane, select **IQ Servers > Schema Objects > Tables**.
5. Select **Tables** or **Proxy Tables**.
6. Select a table or proxy table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table or Proxy Table Properties view appears.

7. In the left pane, select **Triggers**.

Note: **Triggers** does not appear when the selected table is not a system store table.

8. Select one or more triggers from the right pane and click **Delete**.

Note: Use **Shift-click** or **Control-click** to select multiple triggers.

9. Click **Yes** to confirm deletion.

Note: Unlike other wizards launched from the properties view, changes to triggers take effect immediately. You do not need to click **OK** or **Apply** in the properties view to upload the change to the database.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Table Trigger DDL Commands

Display the data description language SQL code for adding a trigger to a table in the database. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Proxy Tables**.
4. Select a table or proxy table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table or Proxy Table Properties view appears.

5. In the left pane, select **Triggers**.

Note: **Triggers** does not appear when the selected table is not a system store table.

6. Select one or more triggers from the right pane and click **Generate DDL**.

Note: Use **Shift-click** or **Control-click** to select multiple triggers.

The DDL view shows the SQL code used to add the selected triggers to the table in the database.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Table Trigger Properties

View or change trigger properties on a table, including the comment and the underlying SQL statement of the trigger.

Prerequisites

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any trigger property page – None required.</p> <p>Modify any trigger property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority, along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.
SAP Sybase IQ 16.0	<p>View any trigger property page – None required.</p> <p>Modify a trigger comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege • ALTER ANY TRIGGER system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege <hr/> <p>Note: ALTER permission on the table is not required to modify a comment.</p> <hr/> <p>Modify any other trigger property:</p> <ul style="list-style-type: none"> • Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TRIGGER system privilege, along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • You own the underlying table of the trigger.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Tables**.
3. Select **Tables** or **Proxy Tables**.
4. Select a table or proxy table from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Table or Proxy Table Properties view appears.

5. In the left pane, select **Triggers**.

Note: **Triggers** does not appear when the selected table is not a system store table.

6. In the right pane, select a trigger and click **Edit**.
The Trigger Properties view appears.
7. View or modify the properties.
 - Any modifications to the properties are saved when either **Apply** or **OK** is clicked
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) The name of the trigger.</p> <p>Dialect – (Read-only) Indicates the dialect of the trigger.</p> <p>Events – (Read-only) Indicates the event which causes the trigger to fire. Valid events are:</p> <ul style="list-style-type: none"> • Insert • Delete • Update • Update with Columns <p>Timing – (Read-only) Indicates when the trigger fires. Valid times are:</p> <ul style="list-style-type: none"> • Before the event (Table only) • Instead of the event • After the event • On a SQL Remote conflict <p>Level – (Read-only) Defines whether the trigger fires at a row or statement level.</p> <p>Comment – An optional text comment on the trigger.</p>
SQL	The SQL statement to be executed when the trigger fires.

8. Click **OK** or **Apply** to close the Trigger properties view.

Note: Unlike other wizards launched from the properties view, changes to triggers take effect immediately. You do not need to click **OK** or **Apply** in the properties view to upload the change to the database.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Table Trigger Privilege Summary

A list of the system privileges and object permissions required to complete the various table trigger tasks on database objects.

Creating a Table Trigger

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority, along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege. • CREATE ANY OBJECT system privilege. Also requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.

Deleting a Table Trigger

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority, along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TABLE system privilege. • You own the underlying table of the trigger.

Generating Table Trigger DDL Commands

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Table Trigger Properties

Database Version	Table Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any trigger property page – None required.</p> <p>Modify any trigger property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority, along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table of the trigger. • You own the underlying table of the trigger.
SAP Sybase IQ 16.0	<p>View any trigger property page – None required.</p> <p>Modify a trigger comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege • ALTER ANY TRIGGER system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege <hr/> <p>Note: ALTER permission on the table is not required to modify a comment.</p> <hr/> <p>Modify any other trigger property:</p> <ul style="list-style-type: none"> • Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TRIGGER system privilege, along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • You own the underlying table of the trigger.

Table Partitions

Dividing large tables into more manageable storage objects, called partitions, can improve performance.

Partitions share the logical attributes of the parent table. Manage partitions individually by placing them in separate dbspaces.

See also

- *Creating a Table* on page 466
- *Creating a Global Temporary Table* on page 474
- *Creating a Proxy Table* on page 479
- *Viewing Table Data in the Execute SQL Window* on page 481
- *Deleting a Table* on page 483
- *Generating Table DDL Commands* on page 484
- *Moving a Table to Another Dbspace* on page 486
- *Validating a System Store Table* on page 488
- *Setting the Primary Key* on page 489
- *Setting a Clustered Index* on page 492
- *Merging Table Data from RLV Store with IQ Main Store* on page 493
- *Calculating the Number of Rows in a Table* on page 495
- *Moving Table Objects to Another Dbspace* on page 497
- *Enabling or Disabling Row-Level Versioning in a Table* on page 499
- *Viewing or Modifying Base Table Properties* on page 501
- *Viewing or Modifying Global Temporary Table Properties* on page 506
- *Viewing and Modifying Proxy Table Properties* on page 512
- *Table Privilege Summary* on page 515
- *Table Columns* on page 528
- *Table Permissions* on page 543
- *Table Constraints* on page 556
- *Table Indexes* on page 586
- *Table Triggers* on page 606

Creating a Hash Partition

Hash partitioning distributes table data to logical partitions for parallel execution, which can enhance join performance on large tables and distributed queries. Hash partitioning maps data to partitions based on partition key values processed by an internal hashing function.

Prerequisites

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	Table owned by self – None required. Table owned by other users – Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.
SAP Sybase IQ 16.0	Requires one of the following: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Very Large Database Management option (IQ_VLDBMGMT).
- The table to be partitioned is empty.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, select the table in the right pane, click the drop-down arrow that appears beside the table name, and select **Properties**.
4. Select **Partitions** and click **New**.
The Create Partition Wizard appears.
5. On the Partition Type tab, specify a hash partition:

Option	Description
What type of partition do you want to create?	Select Hash.

6. Click **Next.**

Hash partition keys are restricted to a maximum of eight columns with a combined declared column width of 5300 bytes or less. You declare the partition key columns; the number and location of the partitions are declared internally.

Partition keys can contain NULL and DEFAULT values. All NULL values are mapped to the same hash partition.

7. Select one or more table columns and click **Add. To remove an added column, select it and click **Remove**.**

Tip: Use **Shift-click** or **Control-click** to select multiple columns.

8. Click **Finish.****9. Click **Apply** or **OK**.****See also**

- *Creating a Range Partition* on page 620
- *Creating a Hash-Range Partition* on page 622
- *Deleting a Partition* on page 624
- *Unpartitioning a Table* on page 625
- *Merging Partitions* on page 627
- *Splitting Partitions* on page 628
- *Moving a Partition* on page 630
- *Managing Column Storage in a Table Partition* on page 632
- *Viewing or Modifying Table Partition Properties* on page 635
- *Table Partition Privilege Summary* on page 639
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Range Partition

Range partitioning divides large tables by a range of partition-key values established for each partition. Range partitioning can shorten backup and restore times, provide a finer level of granularity for data validation, and support tiered storage.

Prerequisites

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • CREATE permission on the dbspaces where the partitions are being created. <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER permission on the table. • You own the table.
SAP Sybase IQ 16.0	<p>Requires one of the following:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspaces along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Very Large Database Management option (IQ_VLDBMGMT).
- If the table to be partitioned contains data, the resulting partitioning must have all rows in the first partition.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, select the table in the right pane, click the drop-down arrow that appears next to the table name, and select **Properties**.
4. Select **Partitions** and click **New**.
The Create Partition Wizard appears.

5. On the Partition Type page, specify a range partition:

Option	Description
What type of partition do you want to create?	Select Range.

6. Click **Next**.

7. On the Partition Key page, specify a column:

Option	Description
Which column do you want to include in the partition key?	<p>Select a table column and click Add.</p> <p>A partition key cannot contain LOB, binary, varbinary, bit, float, double, or real data, or any char or varchar column with a length that exceeds 255 bytes.</p>

8. Click **Next**.

9. On the Partitions page, click **Add**.
The Define a Partition dialog appears.

10. On the Define a Partition dialog, specify the range partition definition:

Option	Description
Specify the name, value and dbspace for the range partition.	<ul style="list-style-type: none"> • Name – Enter a descriptive name for the partition. • Constraint – Less than or equal (\leq) is the only constraint currently supported. • Value – Enter the upper limit value of the partition. • Dbspace – Select the dbspace for the partition from the pull-down.

11. On the Columns page, click **Add** if you want to store any column data in a separate dbspace from the partition. Otherwise, click **Finish**.

If you click **Add**, the Specify Dbspace for a Partition Column page appears.

12. Choose the column, partition, and dbspace from the pull-down and click **OK**.

13. When you have specified all the columns desired, click **Finish**.

See also

- *Creating a Hash Partition* on page 618
- *Creating a Hash-Range Partition* on page 622
- *Deleting a Partition* on page 624
- *Unpartitioning a Table* on page 625
- *Merging Partitions* on page 627
- *Splitting Partitions* on page 628
- *Moving a Partition* on page 630

- *Managing Column Storage in a Table Partition* on page 632
- *Viewing or Modifying Table Partition Properties* on page 635
- *Table Partition Privilege Summary* on page 639
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Hash-Range Partition

Hash-range partitioning is a composite partitioning scheme that subpartitions a hash-partitioned table by range. Hash-range partitioning provides the benefits of hash and range partitioning.

Prerequisites

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• SPACE ADMIN authority, and one of:<ul style="list-style-type: none">• ALTER permission on the table.• You own the table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• ALTER ANY OBJECT system privilege.• CREATE permission on the dbspace along with one of:<ul style="list-style-type: none">• ALTER ANY TABLE system privilege.• ALTER permission on the table.• You own the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Very Large Database Management option (IQ_VLDBMGMT).
- The table to be partitioned is empty.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, select the table in the right pane, click the drop-down arrow that appears next to the table name, and select **Properties**.
4. Select **Partitions** and click **New**.
The Create Partition Wizard appears.

5. On the Partition Type page, specify a hash-range partition:

Option	Description
What type of partition do you want to create?	Select Hash-Range.

6. Click **Next**.

7. On the Partition Key page, specify one or more table columns.

Option	Description
Which column do you want to include in the partition key?	<p>Select one or more table columns and click Add.</p> <p>A partition key cannot contain LOB, binary, varbinary, bit, float, double, or real data, or any char or varchar column with a length that exceeds 255 bytes.</p>

8. Click **Next**.

9. On the Subpartition Key page, specify a column.

Option	Description
Which column do you want to include in the subpartition key?	<p>Select a table column and click Add.</p> <p>A partition key cannot contain LOB, binary, varbinary, bit, float, double, or real data, or any char or varchar column over 255 bytes long.</p>

10. Click **Next**.

11. On the Subpartitions page, specify the range partition definition:

Option	Description
Specify the name, value and dbspace for the range subpartition.	<ul style="list-style-type: none"> Name – Enter a descriptive name for the partition. Constraint – Less than or equal (\leq) is only constraint supported. Value – Enter the upper limit value of the partition. You cannot specify NULL. Dbspace – Select the dbspace for the partition from the pull-down.

12. On the Columns page, click **Add** if you want to store any column data in a separate dbspace from the partition. Otherwise, click **Finish**.

If you click **Add**, the Specify Dbspace for a Partition Column page appears.

13. Choose the column, partition, and dbspace from the pull-down and click **OK**.

14. When you have specified all the columns desired, click **Finish**.

See also

- *Creating a Hash Partition* on page 618
- *Creating a Range Partition* on page 620
- *Deleting a Partition* on page 624
- *Unpartitioning a Table* on page 625
- *Merging Partitions* on page 627
- *Splitting Partitions* on page 628
- *Moving a Partition* on page 630
- *Managing Column Storage in a Table Partition* on page 632
- *Viewing or Modifying Table Partition Properties* on page 635
- *Table Partition Privilege Summary* on page 639
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Partition

Delete one or more partitions from a table.

Prerequisites

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	Table owned by self – None required. Table owned by other users – Requires one of: <ul style="list-style-type: none">• DBA authority.• ALTER permission on the table.
SAP Sybase IQ 16.0	Table owned by self – None required. Table owned by other users – Requires one of: <ul style="list-style-type: none">• ALTER ANY TABLE system privilege.• ALTER ANY OBJECT system privilege.• ALTER permission on the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Unstructured Data Analytics option (IQ_UDA).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, select the table in the right pane, click the drop-down arrow that appears beside the table name, and select **Properties**.
4. Select **Partitions**.
5. Select one or more partitions from the list and click **Delete**.
The selected partitions are removed from the list but they are not yet deleted.
6. Click **Apply** or **OK** to complete the deletion.

See also

- *Creating a Hash Partition* on page 618
- *Creating a Range Partition* on page 620
- *Creating a Hash-Range Partition* on page 622
- *Unpartitioning a Table* on page 625
- *Merging Partitions* on page 627
- *Splitting Partitions* on page 628
- *Moving a Partition* on page 630
- *Managing Column Storage in a Table Partition* on page 632
- *Viewing or Modifying Table Partition Properties* on page 635
- *Table Partition Privilege Summary* on page 639
- *Authenticating a Login Account for a Managed Resource* on page 282

Unpartitioning a Table

Delete all partitions from a table.

Prerequisites

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	Table owned by self – None required. Table owned by other users – Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.
SAP Sybase IQ 16.0	Table owned by self – None required. Table owned by other users – Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Very Large Database Management option (IQ_VLDBMGMT).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, select the table in the right pane, click the drop-down arrow that appears beside the table name, and select **Properties**.
4. Select **Partitions**.
5. Click **Unpartition**.

All partitions are removed from the list but the table is not yet unpartitioned.

6. Click **Apply** or **OK** to complete unpartitioning.

See also

- *Creating a Hash Partition* on page 618
- *Creating a Range Partition* on page 620
- *Creating a Hash-Range Partition* on page 622
- *Deleting a Partition* on page 624
- *Merging Partitions* on page 627
- *Splitting Partitions* on page 628
- *Moving a Partition* on page 630
- *Managing Column Storage in a Table Partition* on page 632
- *Viewing or Modifying Table Partition Properties* on page 635
- *Table Partition Privilege Summary* on page 639
- *Authenticating a Login Account for a Managed Resource* on page 282

Merging Partitions

Merge adjacent range partitions in a table.

Prerequisites

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.
SAP Sybase IQ 16.0	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Very Large Database Management option (IQ_VLDBMGMT).
- Partitions are adjacent and reside in the same dbspace. No data movement is required.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, select the table in the right pane, click the drop-down arrow that appears beside the table name, and select **Properties**.
4. Select **Partitions**.
5. Select a single range or hash-range partition from the list and click **Merge**.
6. Select an adjacent partition from the drop-down list and click **OK**. The drop-down list is empty if no lower or higher partition exists in the same dbspace.
7. Click **Apply** or **OK** to complete the merge.

See also

- *Creating a Hash Partition* on page 618
- *Creating a Range Partition* on page 620

- *Creating a Hash-Range Partition* on page 622
- *Deleting a Partition* on page 624
- *Unpartitioning a Table* on page 625
- *Splitting Partitions* on page 628
- *Moving a Partition* on page 630
- *Managing Column Storage in a Table Partition* on page 632
- *Viewing or Modifying Table Partition Properties* on page 635
- *Table Partition Privilege Summary* on page 639
- *Authenticating a Login Account for a Managed Resource* on page 282

Splitting Partitions

Split range or hash-range partitions in a table.

Prerequisites

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	Table owned by self – None required. Table owned by other users – Requires one of: <ul style="list-style-type: none">• DBA authority.• ALTER permission on the table.• SELECT permission on the table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• SELECT ANY TABLE system privilege.• SELECT permission on table. Also requires one of: <ul style="list-style-type: none">• ALTER ANY OBJECT system privilege.• CREATE permission on the dbspace along with one of:<ul style="list-style-type: none">• ALTER ANY TABLE system privilege.• ALTER permission on the table.• You own the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Very Large Database Management option (IQ_VLDBMGMT).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, select the table in the right pane, click the drop-down arrow that appears beside the table name, and select **Properties**.
4. Select **Partitions**.
5. Select a range or hash-range partition from the list and click **Split**.
6. Specify the name, value, and dbspace for each resulting partition and click **OK**. (You can rename the existing partition, but cannot edit its upper bound or dbspace.)
7. Click **Apply** or **OK** to complete the split.

See also

- *Creating a Hash Partition* on page 618
- *Creating a Range Partition* on page 620
- *Creating a Hash-Range Partition* on page 622
- *Deleting a Partition* on page 624
- *Unpartitioning a Table* on page 625
- *Merging Partitions* on page 627
- *Moving a Partition* on page 630
- *Managing Column Storage in a Table Partition* on page 632
- *Viewing or Modifying Table Partition Properties* on page 635
- *Table Partition Privilege Summary* on page 639
- *Authenticating a Login Account for a Managed Resource* on page 282

Moving a Partition

Move a table partition to another dbspace.

Prerequisites

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority • CREATE permission on the dbspace to which the partition is being moved along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the table.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • One of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace to which the partition is being moved. • Along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the underlying table.

- You have CREATE permission in the new dbspace.
- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Very Large Database Management option (IQ_VLDBMGMT).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, select the table in the right pane, click the drop-down arrow that appears beside the table name, and select **Properties**.

4. Select **Partitions**.
5. Select a partition from the list and click **Move**.
6. Select the new dbspace from the drop-down list and click **OK**.
7. Click **Apply** or **OK** to complete the move.

See also

- *Creating a Hash Partition* on page 618
- *Creating a Range Partition* on page 620
- *Creating a Hash-Range Partition* on page 622
- *Deleting a Partition* on page 624
- *Unpartitioning a Table* on page 625
- *Merging Partitions* on page 627
- *Splitting Partitions* on page 628
- *Managing Column Storage in a Table Partition* on page 632
- *Viewing or Modifying Table Partition Properties* on page 635
- *Table Partition Privilege Summary* on page 639
- *Authenticating a Login Account for a Managed Resource* on page 282

Managing Column Storage in a Table Partition

Store data for individual columns in a range or hash-range partition separately from the dbspace for the partition.

Prerequisites

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority • CREATE permission on the dbspace to which the partition is being moved along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.

Database Version	Table Partition Privileges
SAP Sybase IQ 16.0	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • One of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace to which the partition is being moved. • Along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the underlying table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Very Large Database Management option (IQ_VLDBMGMT).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, select a base table in the right pane, click the drop-down arrow that appears beside the table name, and select **Properties**. (Global temporary tables and proxy tables cannot be partitioned.)
4. Select **Partitions**.
5. Select a hash-range or range partition from the list and click **Edit**.
6. On the Columns page, click **Add** to specify new column storage for an existing partition. Select a column and click **Delete** to remove a column storage definition or **Move** to move the column data to a different dbspace or back to the partition dbspace.

- Moving column data to a new dbspace adds the column to the list of those with separate storage, in Partition Properties and in the Partitions page of Table Properties. Moving the column back to the partition dbspace removes the column from those lists.
- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

7. Click **Apply**.

See also

- *Creating a Hash Partition* on page 618
- *Creating a Range Partition* on page 620
- *Creating a Hash-Range Partition* on page 622
- *Deleting a Partition* on page 624
- *Unpartitioning a Table* on page 625
- *Merging Partitions* on page 627
- *Splitting Partitions* on page 628
- *Moving a Partition* on page 630
- *Viewing or Modifying Table Partition Properties* on page 635
- *Table Partition Privilege Summary* on page 639
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Table Partition Properties

View table partition details or change the table partition details and definition of an existing table partition.

Prerequisites

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority • CREATE permission on the dbspace to which the partition is being moved along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.

Database Version	Table Partition Privileges
SAP Sybase IQ 16.0	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • One of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace to which the partition is being moved. • Along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the underlying table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Very Large Database Management option (IQ_VLDBMGMT).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Tables**.
3. Select **Tables**, select the table in the right pane, click the drop-down arrow that appears beside the table name, and select **Properties**.
4. Select **Partitions**.
5. Select a partition from the list and click **Edit**.
6. View or modify table partition properties. The properties differ depending on the partition type.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

7. Click **OK**.

The Properties view appears.

Hash Partition Properties

Area	Description
General	<p>These properties cannot be edited.</p> <p>Name – Hash (Hash partitions are unnamed.).</p> <p>Type – Hash.</p> <p>Composite – N/A for a hash partition..</p> <p>Partition key – Name of column(s) for the partition key.</p>

Range Partition Properties

Area	Description
General	<p>Name – Name of the range partition.</p> <p>Type – Range.</p> <p>Composite – N/A.</p> <p>Partition key – Name of the column for the partition key.</p> <p>Value – Value of the range partition.</p> <p>DbSPACE – DbSPACE that contains the range partition.</p>
Columns	Column details for columns contained by the range partition. See <i>Managing Column Storage in Table Partition Properties</i> on page 632.

Hash-Range Partition Properties

Area	Description
General	<p>Name – Name of the hash-range partition.</p> <p>Type – Range.</p> <p>Composite – Hash-Range.</p> <p>Partition key – Name of the hash-range partition.</p> <p>Value – Value of the hash-range partition.</p> <p>DbSPACE – DbSPACE that contains the hash-range partition.</p>
Column	Column details for columns contained by the hash- range partition. See <i>Managing Column Storage in Table Partition Properties</i> on page 632.

Tip: You can modify changes in progress before they commit by clicking **Properties** and then making corrections.

8. Click **Apply** or **OK** to complete changes.

See also

- *Creating a Hash Partition* on page 618
- *Creating a Range Partition* on page 620
- *Creating a Hash-Range Partition* on page 622
- *Deleting a Partition* on page 624
- *Unpartitioning a Table* on page 625
- *Merging Partitions* on page 627
- *Splitting Partitions* on page 628
- *Moving a Partition* on page 630
- *Managing Column Storage in a Table Partition* on page 632
- *Table Partition Privilege Summary* on page 639
- *Authenticating a Login Account for a Managed Resource* on page 282

Table Partition Privilege Summary

A list of the system privileges and object permissions required to complete the various table partition tasks.

Creating a Hash Partition

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.
SAP Sybase IQ 16.0	<p>Requires one of the following:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table.

Creating a Range Partition

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • CREATE permission on the dbspaces where the partitions are being created. <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER permission on the table. • You own the table.
SAP Sybase IQ 16.0	<p>Requires one of the following:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspaces along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table.

Creating a Hash-Range Partition

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority, and one of: <ul style="list-style-type: none"> • ALTER permission on the table. • You own the table.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table.

Deleting a Partition

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	Table owned by self – None required. Table owned by other users – Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.
SAP Sybase IQ 16.0	Table owned by self – None required. Table owned by other users – Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

Unpartitioning a Table

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.
SAP Sybase IQ 16.0	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

Merging Partitions

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.
SAP Sybase IQ 16.0	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

Splitting Partitions

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Table owned by self – None required.</p> <p>Table owned by other users – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table. • SELECT permission on the table.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on table. <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace along with one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER permission on the table. • You own the table.

Moving Partitions

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority • CREATE permission on the dbspace to which the partition is being moved along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the table.

Database Version	Table Partition Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • One of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace to which the partition is being moved. • Along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the underlying table.

Managing Column Storage in a Table Partition

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority • CREATE permission on the dbspace to which the partition is being moved along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.

Database Version	Table Partition Privileges
SAP Sybase IQ 16.0	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • One of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace to which the partition is being moved. • Along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the underlying table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

Viewing or Modifying Table Partition Properties

Database Version	Table Partition Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority • CREATE permission on the dbspace to which the partition is being moved along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table.

Database Version	Table Partition Privileges
SAP Sybase IQ 16.0	<p>View any table partition property page – None required.</p> <p>Modify any table partition property pertaining to moving partition location or separate column storage for a partition – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE system privilege. • One of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace to which the partition is being moved. • Along with one of: <ul style="list-style-type: none"> • ALTER permission on the underlying table. • You own the underlying table. <p>Modify any other table partition property:</p> <ul style="list-style-type: none"> • Table owned by self – None required. • Table owned by other users – Requires one of: <ul style="list-style-type: none"> • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table.

See also

- *Creating a Hash Partition* on page 618
- *Creating a Range Partition* on page 620
- *Creating a Hash-Range Partition* on page 622
- *Deleting a Partition* on page 624
- *Unpartitioning a Table* on page 625
- *Merging Partitions* on page 627
- *Splitting Partitions* on page 628
- *Moving a Partition* on page 630
- *Managing Column Storage in a Table Partition* on page 632
- *Viewing or Modifying Table Partition Properties* on page 635

Views

A view is a computed table defined by the result set of its view definition, expressed as a SQL query. You can use views to show database users exactly the information you want to present, in a format you can control.

A *regular view* describes a view that is recomputed each time you reference the view, and the result set is not stored on disk. This is the most commonly used type of view.

A *materialized view* describes a view whose result set is precomputed and materialized on disk similar to the contents of a base table. Materialized views are useful in data warehousing scenarios, where frequent queries of the actual base tables can be extremely expensive.

About Views

A view is a computed table that may be useful for security purposes, and for tailoring the appearance of database information to make data access straightforward. SAP Sybase IQ provides views that allow you to give names to frequently executed **SELECT** commands, saving you from having to repeatedly type them.

Think of views as computed tables. You can use any **SELECT** command in a view definition except commands containing **ORDER BY**. Views can use **GROUP BY** clauses, subqueries, and joins. Disallowing **ORDER BY** in the commands that make up a view is consistent with the fact that rows of a table in a relational database are not stored in any particular order. When you use the view, you can specify an **ORDER BY**.

For example, if you frequently need to list a summary of employees and their departments, create a view called `emp_dept` that looks just like any other table in the `iqdemo` database. You can list everything in a view just as you do from a table.

The information in a view is not stored separately in the database. Each time you refer to a view, SQL executes the associated **SELECT** statement to find the appropriate data.

This also means that if someone modifies the employee table or the department table, the information in the `emp_dept` view is automatically up to date. However, if the **SELECT** command is complicated, it may take a long time for SQL to find the correct information every time you use the view.

You can also use views in more complicated queries, such as queries using joins:

```
SELECT LastName, dept_head_id
FROM emp_dept, department
WHERE emp_dept.Department = department.dept_name
```

See also

- *Creating a View* on page 648
- *Viewing View Data in the Execute SQL Window* on page 650
- *Recompiling and Enabling a View* on page 651

- *Disabling a View* on page 652
- *Deleting a View* on page 653
- *Generating View DDL Commands* on page 655
- *Viewing or Modifying View Properties* on page 656
- *View Privilege Summary* on page 660
- *View Permissions* on page 663
- *View Triggers* on page 679
- *Materialized Views* on page 687

Creating a View

Create a new regular view by defining a SQL query using the Create View wizard.

Prerequisites

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority• RESOURCE authority with SELECT permission on the tables in the view definition to create a view owned by you.
SAP Sybase IQ 16.0	<p>View to be owned by self –</p> <ul style="list-style-type: none">• Requires CREATE VIEW system privilege.• Also requires one of:<ul style="list-style-type: none">• SELECT ANY TABLE system privilege.• SELECT object permission on the underlying tables of the view. <p>View to be owned by any user – Requires one of:</p> <ul style="list-style-type: none">• CREATE ANY VIEW system privilege.• CREATE ANY OBJECT system privilege.• Also requires one of:<ul style="list-style-type: none">• SELECT object permission on the underlying tables of the view.• SELECT ANY TABLE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Views**.
3. Click the arrow next to **View** and select **New**.
The Create View Wizard appears.
4. On the Welcome page, specify

Option	Description
Select a resource for which the view will be created	From the list, select the resource for which the view will be created.
Which user or group do you want to own the view?	From the list, select the user or role/group to own the view.
What do you want to name the view?	Enter a unique name for the new view; maximum of 128 characters.
Comment	Specify a comment for the view.

5. Click **Next**.
6. On the SQL page, define a **SELECT** statement for the view.
7. Click **Next**.
8. On the Options page, select **Enable this view** to enable the view
9. Click **Finish**.

See also

- *About Views* on page 647
- *Viewing View Data in the Execute SQL Window* on page 650
- *Recompiling and Enabling a View* on page 651
- *Disabling a View* on page 652
- *Deleting a View* on page 653
- *Generating View DDL Commands* on page 655
- *Viewing or Modifying View Properties* on page 656
- *View Privilege Summary* on page 660
- *View Permissions* on page 663
- *View Triggers* on page 679
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing View Data in the Execute SQL Window

Execute a **SELECT * FROM** query and display contents of the view in the query results pane of the Execute SQL window.

Prerequisites

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	None required. Query executes with user's current permissions.
SAP Sybase IQ 16.0	None required. Query executes with user's current permissions.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Views > Views**.
3. Select a view from the right pane and either:
 - Click the arrow to the right of the name and select **View Data in SQL** , or
 - From the Administration Console menu bar, select **Resource > View Data in SQL** .

Note: Use **Shift-click** or **Control-click** to select multiple views.

A **SELECT * FROM <view>** query executes.

4. (Optional) Modify the SQL statement and click **Execute** to display different data in the view.
5. Click **Close** to close the Execute SQL view.

See also

- *About Views* on page 647
- *Creating a View* on page 648
- *Recompiling and Enabling a View* on page 651
- *Disabling a View* on page 652
- *Deleting a View* on page 653
- *Generating View DDL Commands* on page 655
- *Viewing or Modifying View Properties* on page 656
- *View Privilege Summary* on page 660
- *View Permissions* on page 663

- *View Triggers* on page 679
- *Authenticating a Login Account for a Managed Resource* on page 282

Recompiling and Enabling a View

Recompile and enable a disabled view to make it available for use by the database server. Enabling a view changes the definition of the view but does not change data inside the view.

Prerequisites

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • All of these: <ul style="list-style-type: none"> • SELECT permission on the underlying tables of the view. • You own the view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the view. • Also require one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the underlying tables of the view.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The view is disabled.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Views**.
3. Select one or more views from the right pane and either:
 - Click the arrow to the right of the name and select **Recompile and Enable**, or
 - From the Administration Console menu bar, select **Resource > Recompile and Enable**.

Note: Use **Shift-click** or **Control-click** to select multiple views.

4. Click **Yes**.

See also

- *About Views* on page 647
- *Creating a View* on page 648
- *Viewing View Data in the Execute SQL Window* on page 650
- *Disabling a View* on page 652
- *Deleting a View* on page 653
- *Generating View DDL Commands* on page 655
- *Viewing or Modifying View Properties* on page 656
- *View Privilege Summary* on page 660
- *View Permissions* on page 663
- *View Triggers* on page 679
- *Authenticating a Login Account for a Managed Resource* on page 282

Disabling a View

Disabling a view makes it unusable, but retains the definition of the view in the database. You can enable and recompile the disabled view at a later time. Disabling a view changes the definition of the view but does not change data inside the view.

Prerequisites

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• You own the view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• ALTER ANY VIEW system privilege.• ALTER ANY OBJECT system privilege.• You own the view.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The view is enabled.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Views**.
3. Select one or more views from the right pane and either:
 - Click the arrow to the right of the name and select **Disable**, or
 - From the Administration Console menu bar, select **Resource > Disable**.

Note: Use **Shift-click** or **Control-click** to select multiple views.

4. Click **Yes**.

See also

- *About Views* on page 647
- *Creating a View* on page 648
- *Viewing View Data in the Execute SQL Window* on page 650
- *Recompiling and Enabling a View* on page 651
- *Deleting a View* on page 653
- *Generating View DDL Commands* on page 655
- *Viewing or Modifying View Properties* on page 656
- *View Privilege Summary* on page 660
- *View Permissions* on page 663
- *View Triggers* on page 679
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a View

Delete an enabled or disabled view to remove it from the database. Deleting a view deletes the definition of the view. All data related to the view are virtual, and remain in the underlying tables after deletion.

Prerequisites

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the view.

Database Version	View Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY VIEW system privilege. • DROP ANY OBJECT system privilege. • You own the view.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Views**.
3. Select one or more views from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple views.

4. Click **Yes** to confirm deletion.

See also

- *About Views* on page 647
- *Creating a View* on page 648
- *Viewing View Data in the Execute SQL Window* on page 650
- *Recompiling and Enabling a View* on page 651
- *Disabling a View* on page 652
- *Generating View DDL Commands* on page 655
- *Viewing or Modifying View Properties* on page 656
- *View Privilege Summary* on page 660
- *View Permissions* on page 663
- *View Triggers* on page 679
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating View DDL Commands

Display the data description language SQL code for adding a view to the database. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Views**.
3. Select one or more views from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Note: Use **Shift-click** or **Control-click** to select multiple views.

The DDL view shows the SQL code used to add the selected views to the database.

See also

- *About Views* on page 647
- *Creating a View* on page 648
- *Viewing View Data in the Execute SQL Window* on page 650
- *Recompiling and Enabling a View* on page 651
- *Disabling a View* on page 652
- *Deleting a View* on page 653
- *Viewing or Modifying View Properties* on page 656
- *View Privilege Summary* on page 660
- *View Permissions* on page 663
- *View Triggers* on page 679
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying View Properties

View or change view properties including the comment, SQL view definition (including the column definition), and permissions. Modifying a view changes the definition of the view but does not change data inside the view.

Prerequisites

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any view property page – None required.</p> <p>Modify view permissions – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• Administrative rights over the permission.• You own the database object. <p>Modify any other view property except those relating to triggers – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• You own the view. <p>For privileges relating to triggers, see:</p> <ul style="list-style-type: none">• <i>View Trigger Privilege Summary</i> on page 685

Database Version	View Privileges
SAP Sybase IQ 16.0	<p>View any view property page – None required.</p> <p>Modify view permissions – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object. <p>Modify a view comment – Requires any one of:</p> <ul style="list-style-type: none"> • CREATE ANY VIEW system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY VIEW system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the view. <p>Modify any other view property, except those relating to triggers – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the view. <p>For privileges relating to view triggers, see:</p> <ul style="list-style-type: none"> • <i>View Trigger Privilege Summary</i> on page 685

- (Modifying properties only) In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Views**.
3. Select a view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The View Properties view appears.

4. View or modify the properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.

- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) The name of the view.</p> <p>Owner – (Read-only) The owner of the view.</p> <p>Database – (Read-only) The name of the database the view was created for.</p> <p>Status – Current status of the view. Valid statuses are:</p> <ul style="list-style-type: none"> • Valid • Disabled <p>Recompile and Enable Now – Allows you to enabled a disabled view.</p> <p>Disable Now – Allows you to disable an enabled view.</p> <p>Comment – Enter a comment on the view.</p>
SQL	View the SELECT statement for the view.
Columns (Read-only)	<p>Name – Column name.</p> <p>ID – Column ID.</p> <p>Data Type – Column Data type.</p> <p>Allows null – Indicates if the column accepts null values. Either Yes or No.</p>
Triggers	<p>(System store tables only.)</p> <p>See <i>View Triggers</i> on page 679 for details and required privileges and permissions.</p>
Data (Read-only)	<p>Note: For 15.3 and 15.4, requires SELECT permission on the underlying table to view data. For 16.0, requires the SELECT ANY TABLE system privilege to view data.</p> <p>Displays the first 500 rows of data.</p>
Permissions	See <i>View Permissions</i> on page 663 for details and required privileges and permissions.

Area	Description
Referenced Objects (Read-only)	<p>Name – Table name.</p> <p>Owner – Table owner.</p> <p>Object Type – Referenced object type (Table, for example).</p> <p>Referenced Column – Column ID.</p> <p>Dependency Type – Indicates Direct or Indirect dependency.</p>
Dependent Views (Read-only)	<p>Name – View name.</p> <p>Owner – View owner.</p> <p>View Type – View type.</p> <p>Dependency Type – Indicates Direct or Indirect dependency.</p>

5. Click **OK**.

See also

- *About Views* on page 647
- *Creating a View* on page 648
- *Viewing View Data in the Execute SQL Window* on page 650
- *Recompiling and Enabling a View* on page 651
- *Disabling a View* on page 652
- *Deleting a View* on page 653
- *Generating View DDL Commands* on page 655
- *View Privilege Summary* on page 660
- *View Permissions* on page 663
- *View Triggers* on page 679
- *Authenticating a Login Account for a Managed Resource* on page 282

View Privilege Summary

A list of the system privileges and object permissions required to complete the various view tasks.

Creating a View

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority • RESOURCE authority with SELECT permission on the tables in the view definition to create a view owned by you.
SAP Sybase IQ 16.0	<p>View to be owned by self –</p> <ul style="list-style-type: none"> • Requires CREATE VIEW system privilege. • Also requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT object permission on the underlying tables of the view. <p>View to be owned by any user – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY VIEW system privilege. • CREATE ANY OBJECT system privilege. • Also requires one of: <ul style="list-style-type: none"> • SELECT object permission on the underlying tables of the view. • SELECT ANY TABLE system privilege.

Viewing View Data in the Execute SQL Window

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	None required. Query executes with user's current permissions.
SAP Sybase IQ 16.0	None required. Query executes with user's current permissions.

Recompiling and Enabling a View

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • All of these: <ul style="list-style-type: none"> • SELECT permission on the underlying tables of the view. • You own the view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the view. • Also require one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the underlying tables of the view.

Disabling a View

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the view.

Deleting a View

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the view.

Database Version	View Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY VIEW system privilege. • DROP ANY OBJECT system privilege. • You own the view.

Generating View DDL Commands

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying View Properties

Database Version	View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any view property page – None required.</p> <p>Modify view permissions – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object. <p>Modify any other view property except those relating to triggers – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the view. <p>For privileges relating to triggers, see:</p> <ul style="list-style-type: none"> • <i>View Trigger Privilege Summary</i> on page 685

Database Version	View Privileges
SAP Sybase IQ 16.0	<p>View any view property page – None required.</p> <p>Modify view permissions – Requires one of:</p> <ul style="list-style-type: none"> • <code>MANAGE ANY OBJECT PRIVILEGE</code> system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object. <p>Modify a view comment – Requires any one of:</p> <ul style="list-style-type: none"> • <code>CREATE ANY VIEW</code> system privilege. • <code>CREATE ANY OBJECT</code> system privilege. • <code>ALTER ANY VIEW</code> system privilege. • <code>ALTER ANY OBJECT</code> system privilege. • <code>COMMENT ANY OBJECT</code> system privilege. • You own the view. <p>Modify any other view property, except those relating to triggers – Requires one of:</p> <ul style="list-style-type: none"> • <code>ALTER ANY VIEW</code> system privilege. • <code>ALTER ANY OBJECT</code> system privilege. • You own the view. <p>For privileges relating to view triggers, see:</p> <ul style="list-style-type: none"> • <i>View Trigger Privilege Summary</i> on page 685

See also

- *About Views* on page 647
- *Creating a View* on page 648
- *Viewing View Data in the Execute SQL Window* on page 650
- *Recompiling and Enabling a View* on page 651
- *Disabling a View* on page 652
- *Deleting a View* on page 653
- *Generating View DDL Commands* on page 655
- *Viewing or Modifying View Properties* on page 656
- *View Permissions* on page 663
- *View Triggers* on page 679

View Permissions

Grant or revoke view permissions to users and roles.

See also

- *About Views* on page 647
- *Creating a View* on page 648
- *Viewing View Data in the Execute SQL Window* on page 650
- *Recompiling and Enabling a View* on page 651
- *Disabling a View* on page 652
- *Deleting a View* on page 653
- *Generating View DDL Commands* on page 655
- *Viewing or Modifying View Properties* on page 656
- *View Privilege Summary* on page 660
- *View Triggers* on page 679

About the View Permissions List

The View permissions list displays details on the specific object permissions directly granted to users or roles for a single view.

There are four object permissions for views or materialized views, which can be granted with or without administrative rights:

- SELECT
- INSERT
- DELETE
- UPDATE

These object permissions can be granted in several ways:

- You own the object.
- You are granted the `MANAGE ANY OBJECT PRIVILEGE` system privilege.
- You have been indirectly granted specific permissions through membership in a role to which permissions have been directly or indirectly granted.
- You have been directly granted specific permissions.

Users or roles with object ownership or the `MANAGE ANY OBJECT PRIVILEGE` system privilege are automatically granted all possible object permissions with administrative rights.

Object permissions can be granted with or without administrative rights. When granted without administrative rights, the grantee can perform authorized tasks requiring the permission, but cannot in turn grant the permission to another user or role. When granted with administrative rights (With grant option), the grantee can do both.

The permissions list only lists those permissions granted directly to user or roles. The list indicates who the permissions are granted to whom (grantee), by who (grantor), and the permissions and their corresponding administrative rights. The permissions list does not list object permissions obtained through ownership, the `MANAGE ANY SYSTEM OBJECT` system privilege, or role membership.

						Grant...	Revoke
Grantee	grantor	Select	Insert	Delete	Update		
Manager1	Manager1	✓ ↔	✓ ↔	✓ ↔	✓ ↔		
User2	Manager1	✓		✓			
User2	User1		✓ ↔				

Legend:

- ✓ Permission granted with no administrative rights
- ✓ ↔ Permission granted with administrative rights

When granted to a role, permissions, including administrative rights, are inherited by all members of the role. The role, not the users indirectly granted the permissions through inheritance, appear on the permissions list.

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the SELECT permission with the With grant option. UserA grants SELECT to UserB with the With grant option. UserB grants SELECT to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the SELECT permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

Permissions can be granted on the same view or materialized view, to the same grantee, by multiple grantors, resulting in the same grantee appearing multiple times on the list. If the same permission is granted to the same grantee, with and without administrative rights, the grant with the administrative right takes precedence.

Grantee	grantor	Select	Insert	Delete	Update
Manager1	Manager1	✓ ↔	✓ ↔	✓ ↔	✓ ↔
User2	Manager1	✓	✓	✓	
User2	User1		✓ ↔		

When revoking a permission granted multiple times, the permission is revoked from all instances, regardless of administrative rights. For example, Manager1 grants User2 INSERT with administrative rights. User1 also grants INSERT to User2, but without administrative rights. Regardless of which instance of INSERT is revoked, both instances of INSERT are revoked for User2.

Following the View Permission Grant Trail

Before revoking a grantee's permission, you need to identify grantees directly or indirectly granted the permission from the original grantee.

The grant chain traces how a grantee has in turn granted a permission to other grantees.

Consider the following:

- Bob is granted all permissions with administrative rights.
- Bob grants Joe SELECT permission without administrative rights. Bob also grants Jane SELECT and INSERT permissions with administrative rights.
- Jane grants Mike and Joe SELECT and DELETE permissions with administrative rights. Jane also grants Beth and Mary SELECT permissions without administrative rights.

Note: Joe has now been granted the SELECT permission twice, with different administrative rights, by different grantors.

- Joe grants Beth SELECT permission without administrative rights

Note: Beth has now been granted the SELECT permission twice, by different grantors.

- Mike grants Sarah SELECT and UPDATE permission with administrative rights. Mike also grants Alice SELECT permission without administrative rights.
- Sarah grants Alex, Beth, and Role1 SELECT and UPDATE permissions without administrative rights.

Note: Beth has now been granted the SELECT permission multiple times, by different grantors.

The permissions list would appear similar to:

							Grant...	Revoke
Grantee	1 ▲	grantor	Select	Insert	Delete	Update		
Alex		Sarah	✓			✓		
Alice		Mike	✓					
Beth		Jane	✓					
Beth		Joe	✓					
Beth		Sarah	✓			✓		
Bob		Manager	✓ ↔	✓ ↔	✓ ↔	✓ ↔		
Jane		Bob	✓ ↔	✓ ↔				
Joe		Bob	✓					
Joe		Jane	✓ ↔		✓ ↔			
Mary		Jane	✓					
Mike		Jane	✓ ↔		✓ ↔			
Role1		Sarah	✓			✓		
Sarah		Mike	✓ ↔			✓ ↔		

You want to revoke SELECT permission from Jane. To determine the potential impact on other users and roles, do the following:

Tip: For complex grant trails, create a tree diagram to visually track the grant chain.

1. Sort the list by Grantor and locate all instances of administrative grants of SELECT by Jane.

Permissions						
Grantee		1 grantor	1 ▲	Select	Insert	Delete
Jane	Bob			✓ ↔	✓ ↔	
Joe	Bob			✓		
Mike	Jane			✓ ↔		✓ ↔
Joe	Jane			✓ ↔		✓ ↔
Beth	Jane			✓		
Mary	Jane			✓		
Beth	Joe			✓		
Bob	Manager			✓ ↔	✓ ↔	✓ ↔
Alice	Mike			✓		
Sarah	Mike			✓ ↔		✓ ↔
Beth	Sarah			✓		✓
Alex	Sarah			✓		✓
Role1	Sarah			✓		✓

Note: There are four instances of Jane granting permissions. Since we are revoking the SELECT permission only, only those grants involving the SELECT permission will be impacted. Therefore, revoking Jane's SELECT permission will also revoke the permission from Mary, Mike, and Beth. Of the SELECT permissions, we need to follow those involving administrative rights.

- 2. Locate Mike in the Grantor column.**

Permissions						
Grantee	grantor	1 ▲	Select	Insert	Delete	Update
Jane	Bob		✓ ↔	✓ ↔		
Joe	Bob		✓			
Mike	Jane		✓ ↔		✓ ↔	
Joe	Jane		✓ ↔		✓ ↔	
Beth	Jane		✓			
Mary	Jane		✓			
Beth	Joe		✓			
Bob	Manager		✓ ↔	✓ ↔	✓ ↔	✓ ↔
Alice	Mike	2	✓			
Sarah	Mike		✓ ↔			✓ ↔
Beth	Sarah		✓			✓
Alex	Sarah		✓			✓
Role1	Sarah		✓			✓

Note: Mike granted SELECT to Sarah and Alice. Both were granted the SELECT permission as an indirect (once removed) result of Jane. It does not matter whether the grant included administrative rights. Therefore, their SELECT permission will also be revoked when Jane's is revoked. Since Alice was granted SELECT without administrative rights, her grant chain ends. Since Sarah was granted SELECT with administrative rights, her grant chain continues.

- 3. Locate Sarah in the Grantor column.**

						Grant...	Revoke
Grantee	grantor	1 ▲	Select	Insert	Delete	Update	
Jane	Bob		✓ ↔	✓ ↔			
Joe	Bob		✓				
Mike	Jane		✓ ↔		✓ ↔		
Joe	Jane		✓ ↔		✓ ↔		
Beth	Jane		✓				
Mary	Jane		✓				
Beth	Joe		✓				
Bob	Manager		✓ ↔	✓ ↔	✓ ↔	✓ ↔	
Alice	Mike		✓				
Sarah	Mike		✓ ↔			✓ ↔	
Beth	Sarah		✓			✓	
Alex	Sarah 3		✓			✓	
Role1	Sarah		✓			✓	

Note: Sarah granted SELECT to Beth and Alex. Both were granted the SELECT permission as an indirect (twice removed) result of Jane. Again, administrative rights do not matter, and since neither grant was with administrative rights, the grant chain ends.

To summarize, revoking Jane's SELECT permission revokes the permission from Mike, Joe, Beth, and Mary, through direct granting or permissions by Jane, but also revokes the permission from Alice, Sarah, Alex, and Role1 as a result of indirect from Jane. The permissions list after revoking Jane's SELECT permission would appear similar to:

							Grant...	Revoke
Grantee	grantor	1 ▲	Select	Insert	Delete	Update		
Jane	Bob		✓ ↔	✓ ↔				
Joe	Bob		✓					
Mike	Jane		✓ ↔		✓ ↔			
Joe	Jane		✓ ↔		✓ ↔			
Beth	Jane		✓					
Mary	Jane		✓					
Beth	Joe		✓					
Bob	Manager		✓ ↔	✓ ↔	✓ ↔	✓ ↔		
Alice	Mike		✓					
Sarah	Mike		✓ ↔			✓ ↔		
Beth	Sarah		✓			✓		
Alex	Sarah		✓			✓		
Role1	Sarah		✓			✓		

It is important to note that it is possible for a user to retain an "identified" permission after revoke it the same permission was granted by multiple grantors. In this scenario, both Bob and Jane granted the SELECT permission to Joe, so Joe retains the SELECT permission granted by Bob. If a grantee has been granted multiple permissions, only those permissions explicitly selected are revoked. In this scenario, only the SELECT permission was revoked from Joe. The DELETE permission remains granted, even though it was also granted by Jane.

							Grant...	Revoke
Grantee	grantor		Select	Insert	Delete	Update		
Alex	Sarah					✓		
Beth	Sarah					✓		
Bob	Manager		✓ ↔	✓ ↔	✓ ↔	✓ ↔		
Jane	Bob			✓ ↔				
Joe	Bob		✓					
Joe	Jane				✓ ↔			
Mike	Jane				✓ ↔			
Role1	Sarah					✓		
Sarah	Mike					✓ ↔		

Granting View Permissions

Grant view permissions to users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• Administrative rights over the permission.• You own the database object.
SAP Sybase IQ	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You have administrative rights (with grant option) to the permission.• You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Views > Views**.
3. Select a view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The View Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, click **Grant**.

The Grant Permission Wizard appears.
6. On the Welcome page, indicate whether the permission is being granted to a user or role.
7. Click **Next**.

8. On the Grantees page, select one or more users or roles. Click the box in the header row to select all available users or roles.
9. Click **Next**.
10. On the Permissions page, select one or more permissions. Click the box in the header row to select all available permissions.
11. Click **Next**.
12. (Optional) Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

13. Click **Finish**.

14. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Revoking View Permissions

Remove view permissions from users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object.
SAP Sybase IQ	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right

only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the **SELECT** permission with the **With grant option**. UserA grants **SELECT** to UserB with the **With grant option**. UserB grants **SELECT** to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the **SELECT** permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Views > Views**.
3. Select a view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The View Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, select a user or role granted permissions to be revoked, and click **Revoke**.
A list of permissions currently granted (regardless of administrative rights) appears..
6. Select one or more permissions to revoke. Click the box in the header row to select all available permissions.

Warning! Revoking permissions may result in unexpected revocation from other users or groups. See *Following the View Permission Grant Trail*.

7. Click **Finish**.
8. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Removing Administrative Rights Only from a View Permission

Remove administrative rights only from a granted view permission.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are logged on as the original grantor of the permission with administrative rights to be removed.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Views > Views**.
3. Select a view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The View Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, click **Grant**.
6. On the Welcome page, indicate whether the grantee is a user or role.
7. Click **Next**.
8. On the Grantees page, select the grantee.
9. Click **Next**.
10. On the Permissions page, select the permissions from which the administrative rights are being revoked.
11. Click **Finish**.
12. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Adding Administrative Rights to a Granted View Permission

Add administrative rights only to a granted view permission.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You have administrative rights to the permission being modified.• You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the Administration Console, expand **IQ Servers > Schema Objects > Views > Views**.
3. Select a view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The View Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, select the grantee to have administrative rights granted on a permission. If the grantee appears on the list multiple times with the same permission granted, it does not matter which instance is selected.
6. In the right pane, click **Grant**.
7. On the Welcome page, indicate whether the grantee is a user or role.
8. Click **Next**.
9. On the Grantees page, select the grantee.
10. Click **Next**.
11. On the Permissions page, select the permission to which administrative rights are to be granted.
12. Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

13. Click **Finish**.
14. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

View Permissions Privilege Summary

A list of the system privileges and object permissions required to complete the various view permission tasks.

Grant and Revoke Permissions on a View

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object.
SAP Sybase IQ	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

Adjust Administration Permissions on a View

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

View Triggers

Trigger management includes the creation, modification and deletion of triggers on a database object. A trigger is a special form of stored procedure that executes automatically when a statement that modifies data displayed in a view is executed.

Triggers can only fire against system store tables, but a view can reference multiple tables from the IQ main or system stores. Therefore, triggers that references tables from both stores will fire, but only against system store tables.

See also

- *About Views* on page 647
- *Creating a View* on page 648
- *Viewing View Data in the Execute SQL Window* on page 650
- *Recompiling and Enabling a View* on page 651
- *Disabling a View* on page 652
- *Deleting a View* on page 653
- *Generating View DDL Commands* on page 655
- *Viewing or Modifying View Properties* on page 656
- *View Privilege Summary* on page 660
- *View Permissions* on page 663

Creating a View Trigger

Create a new trigger on a view in the system store.

Prerequisites

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority and you own the underlying view of the trigger.

Database Version	View Trigger Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege. • CREATE ANY OBJECT system privilege. <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY VIEW system privilege. • You own the underlying view of the trigger.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The view on which the trigger resides only references system store tables.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Views**.
3. Select a view from the right pane on which to create the trigger and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Views Properties view appears.

4. In the left pane, select **Triggers**.
5. In the right pane, click **New**.
The Create Trigger Wizard appears.
6. On the Welcome page, enter a unique name for the new trigger.
7. Click **Next**.
8. On the Events page, select one or more events to cause the trigger to fire.
9. Click **Next**.
10. On the Level page, indicate whether the trigger is to fire at the row or statement level.
11. Click **Next**.
12. On the SQL page, enter the statement to be executed when the trigger fires. Triggers do not fire after the execution of LOAD TABLE, TRUNCATE, or WRITETEXT statements.
The statement window provides a template on which to build the trigger statement. The parameters displayed are based on the options selected in the preceding pages. Once you have made any changes in the statement window, if you return to any of the preceding

pages and change any option, when you return to the SQL page, the contents of the statement window is overwritten with the base template; any customizations are lost.

13. Click **Next**.

14. On the Comment page, enter an optional comment.

15. Click **Finish**.

Note: Unlike other wizards launched from the properties view, changes to triggers take effect immediately. You do not need to click **OK** or **Apply** in the properties view to upload the change to the database.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a View Trigger

Delete triggers from a view.

Prerequisites

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the underlying view of the trigger.
SAP Sybase IQ 16.0	Requires ALTER permission on the underlying view of the trigger by virtue of any one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY VIEW system privilege. • You own the underlying view of the trigger.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Views**.
3. Select a view from the right pane on which to create the trigger and either:
 - Click the arrow to the right of the name and select **Properties**, or

- From the Administration Console menu bar, select **Resource > Properties**.

The Views Properties view appears.

4. In the left pane, select **Triggers**.
5. Select one or more triggers from the right pane and click **Delete**.

Note: Use **Shift-click** or **Control-click** to select multiple triggers.

6. Click **Yes** to confirm deletion.

Note: Unlike other wizards launched from the properties view, changes to triggers take effect immediately. You do not need to click **OK** or **Apply** in the properties view to upload the change to the database.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Generating View Trigger DDL Commands

Display the data description language SQL code for adding a trigger to a view in the database. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Views**.
3. Select a view from the right pane on which to create the trigger and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Views Properties view appears.

4. In the left pane, select **Triggers**.
5. Select one or more triggers from the right pane and click **Generate DDL**.

Note: Use **Shift-click** or **Control-click** to select multiple triggers.

The DDL view shows the SQL code used to add the selected triggers to the view in the database.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying View Trigger Properties

View or change trigger properties on a view, including the comment and the underlying SQL statement of the trigger.

Prerequisites

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View trigger properties only – None required.</p> <p>Modify trigger comment or properties – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority and you own the underlying view of the trigger.
SAP Sybase IQ 16.0	<p>View any trigger property page – None required.</p> <p>Modify a trigger comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege • ALTER ANY TRIGGER system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege <hr/> <p>Note: ALTER permission on the view is not required to modify a comment.</p> <hr/> <p>Modify any other trigger property:</p> <ul style="list-style-type: none"> • Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TRIGGER system privilege, along with one of: <ul style="list-style-type: none"> • ALTER ANY VIEW system privilege. • You own the underlying view of the trigger.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Views**.
3. Select a view from the right pane on which to create the trigger and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Views Properties view appears.

4. In the left pane, select **Triggers**.
5. In the right pane, select a trigger and click **Edit**.
The Trigger Properties view appears.
6. View or modify the properties.
 - Any modifications to the properties are saved when either **Apply** or **OK** is clicked
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) The name of the trigger.</p> <p>Dialect – (Read-only) Indicates the dialect of the trigger.</p> <p>Events – (Read-only) Indicates the event which causes the trigger to fire. Valid events are:</p> <ul style="list-style-type: none"> • Insert • Delete • Update <p>Tining – (Read-only) Indicates when the trigger fires. Valid times are:</p> <ul style="list-style-type: none"> • Instead of the event <p>Level – (Read-only) Defines whether the trigger fires at a row or statement level.</p> <p>Comment – An optional text comment on the trigger.</p>
SQL	The SQL statement to be executed when the trigger fires.

7. Click **OK** or **Apply** to close the Trigger properties view.

Note: Unlike other wizards launched from the properties view, changes to triggers take effect immediately. You do not need to click **OK** or **Apply** in the properties view to upload the change to the database.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

View Trigger Privilege Summary

A list of the system privileges and object permissions required to complete the various view trigger tasks on database objects.

Creating a View Trigger

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority and you own the underlying view of the trigger.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege. • CREATE ANY OBJECT system privilege. Also requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY VIEW system privilege. • You own the underlying view of the trigger.

Deleting a View Trigger

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the underlying view of the trigger.

Database Version	View Trigger Privileges
SAP Sybase IQ 16.0	<p>Requires ALTER permission on the underlying view of the trigger by virtue of any one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY VIEW system privilege. • You own the underlying view of the trigger.

Generating View Trigger DDL Commands

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying View Trigger Properties

Database Version	View Trigger Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View trigger properties only – None required.</p> <p>Modify trigger comment or properties – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority and you own the underlying view of the trigger.

Database Version	View Trigger Privileges
SAP Sybase IQ 16.0	<p>View any trigger property page – None required.</p> <p>Modify a trigger comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TRIGGER system privilege • ALTER ANY TRIGGER system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege <hr/> <p>Note: ALTER permission on the view is not required to modify a comment.</p> <hr/> <p>Modify any other trigger property:</p> <ul style="list-style-type: none"> • Requires one of: <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • ALTER ANY TRIGGER system privilege, along with one of: <ul style="list-style-type: none"> • ALTER ANY VIEW system privilege. • You own the underlying view of the trigger.

Materialized Views

A materialized view is a view whose result set has been computed and stored on disk, similar to a base table. Conceptually, a materialized view is both a view (it has a query specification stored in the catalog) and a table (it has persistent materialized rows). Materialized views are only supported for system store (IQ catalog store) tables.

Many operations that you perform on tables can be performed on materialized views as well. For example, you can build indexes on materialized views. Column statistics are generated and maintained for materialized views in exactly the same manner as for tables.

Consider using materialized views for frequently executed, expensive queries, such as those involving intensive aggregation and join operations. Materialized views provide a queryable structure in which to store aggregated, joined data. Materialized views are designed to improve performance in environments where the database is large, and where frequent queries result in repetitive aggregation and join operations on large amounts of data. For example, materialized views are ideal for use with data warehousing applications.

Materialized views are precomputed using data from the base tables that they refer to. Materialized views are read only; you cannot perform data-altering operations such as **INSERT**, **LOAD**, **DELETE**, and **UPDATE** on them.

While you can create indexes on materialized views, you cannot create keys, constraints, triggers, or articles on them.

There are two types of materialized views:

- **Manual views** – a manual materialized view, or manual view, is a materialized view with a refresh type defined as **MANUAL REFRESH**. Data in manual views can become stale because manual views are not refreshed until a refresh is explicitly requested, for example by using the **REFRESH MATERIALIZED VIEW** statement or the **sa_refresh_materialized_views** system procedure. By default, when you create a materialized view, it is a manual view.

A manual view is considered stale as soon as any of the underlying tables change, even if the change does not impact data in the materialized view. You can determine whether a manual view is considered stale by examining the `DataStatus` value returned by the **sa_materialized_view_info** system procedure. If `S` is returned, the manual view is stale.

- **Immediate views** – an immediate materialized view, or immediate view, is a materialized view with a refresh type defined as **IMMEDIATE REFRESH**. Data in an immediate view is automatically refreshed when changes to the underlying tables affect data in the view. If changes to the underlying tables do not impact data in the view, the view is not refreshed.

When an immediate view is refreshed, only the rows that need to be changed are acted upon. This is different from refreshing a manual view, where all data is dropped and recreated for a refresh.

You can change a manual view to an immediate view, and vice versa. However, the process for changing from a manual view to an immediate view has more steps. Changing the refresh type for a materialized view can impact the status and properties of the view, especially when you change a manual view to an immediate view.

See also

- *About Views* on page 647

Creating a Materialized View

Define a SQL query, using the Create Materialized View wizard, to create a new materialized view in the system store (IQ catalog store).

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Materialized view to be owned by self –</p> <ul style="list-style-type: none"> Requires RESOURCE authority with SELECT permission on tables in the view definition. Requires CREATE permission on the selected dbspace to create a view owned by you. <p>Materialized view to be owned by any user – Requires DBA authority.</p>
SAP Sybase IQ 16.0	<p>Materialized view to be owned by self –</p> <ul style="list-style-type: none"> Requires CREATE MATERIALIZED VIEW system privilege. Also requires one of: <ul style="list-style-type: none"> CREATE ANY OBJECT system privilege. CREATE object permission on the dbspace where the materialized view is being created. Also requires one of: <ul style="list-style-type: none"> SELECT ANY TABLE system privilege. SELECT object permission on the underlying tables of the materialized view. <p>Materialized view to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE object permission on the dbspace where the materialized view is being created. Also requires one of: <ul style="list-style-type: none"> CREATE ANY MATERIALIZED VIEW system privilege. CREATE ANY OBJECT system privilege. And also requires one of: <ul style="list-style-type: none"> SELECT ANY TABLE system privilege. SELECT object permission on the underlying tables of the materialized view.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

Materialized views are only supported for system store (IQ catalog store) tables.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Click the arrow next to **Materialized Views** and select **New**.
The Create Materialized View Wizard appears.
4. On the Welcome page, specify

Option	Description
Select a resource for which the materialized view will be created	From the list, select the resource for which the materialized view will be created.
Which user or group do you want to own the materialized view?	From the list, select the user or role/group to own the materialized view.
What do you want to name the materialized view?	Enter a unique name for the new materialized view; maximum of 128 characters.
Comment	Specify a comment for the materialized view.

5. Click **Next**.
6. On the SQL page, define a **SELECT** statement for the materialized view.
7. Click **Next**.
8. On the Dbspace page, specify the dbspace that will be used to store the materialized view.
9. Click **Next**.
10. On the Free Space page, specify the amount of free space you want to reserve for each materialized view page.
11. Click **Next**.
12. On the Options page, specify:

Option	Description
Enable this materialized view	Select option to enable.
Enable use of this materialized view in optimization	Select option to enable.

13. Click **Finish**.

See also

- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692

- *Truncating Materialized View Data* on page 695
- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing Materialized View Data in the Execute SQL Window

Execute a **SELECT * FROM** query and display contents of the materialized view in the query results pane of the Execute SQL window.

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	None required. Query executes with user's current permissions.
SAP Sybase IQ 16.0	None required. Query executes with user's current permissions.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **View Data in SQL** , or
 - From the Administration Console menu bar, select **Resource > View Data in SQL** .

Note: Use **Shift-click** or **Control-click** to select multiple materialized views.

A **SELECT * FROM <materialized view>** query executes.

4. (Optional) Modify the SQL statement and click **Execute** to display different data in the materialized view.
5. Click **Close** to close the Execute SQL view.

See also

- *Creating a Materialized View* on page 689
- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695
- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282

Refreshing Materialized View Data

Refresh materialized view data to apply any modifications to underlying base tables to the view.

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority. Also requires both of: <ul style="list-style-type: none">• INSERT permission on the underlying tables of the materialized view or you own the materialized view.• SELECT permission on the underlying tables of the materialized view or you own the underlying tables of the materialized view.

Database Version	Materialized View Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • INSERT ANY TABLE system privilege. • INSERT permission on the materialized view. • You own the materialized view. <p>Also requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the underlying tables of the materialized view. • You own the underlying tables of the materialized view.

- The SAP Sybase IQ resource is authenticated and running.
- The materialized view is enabled.

Task

Materialized view data is read-only. Materialized views are only supported for system store (IQ catalog store) tables.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select one or more materialized views from the right pane and either:
 - Click the arrow to the right of the name and select **Refresh Data**, or
 - From the Administration Console menu bar, select **Resource > Refresh Data**.

Tip: Use **Shift-click** or **Control-click** to select multiple materialized views.

4. Verify that the list of materialized views to be refreshed is correct and click **Yes**.
5. Select an isolation level.

Level	Description
Read uncommitted (level 0)	<ul style="list-style-type: none"> • Read permitted on row with or without write lock • No read locks are applied • No guarantee that concurrent transaction will not modify row or roll back changes to row • Corresponds to table hints NOLOCK and READUNCOMMITTED • Allow dirty reads, non-repeatable reads, and phantom rows

Level	Description
Read committed (level 1)	<ul style="list-style-type: none"> • Read only permitted on row with no write lock • Read lock acquired and held for read on current row only, but released when cursor moves off the row • No guarantee that data will not change during transaction • Corresponds to table hint READCOMMITTED • Prevent dirty reads • Allow non-repeatable reads and phantom rows
Repeatable read (level 2)	<ul style="list-style-type: none"> • Read only permitted on row with no write lock • Read lock acquired as each row in the result set is read, and held until transaction ends • corresponds to table hint REPEATABLEREAD • Prevent dirty reads and non-repeatable reads • Allow phantom rows
Serializable (level 3)	<ul style="list-style-type: none"> • Read only permitted on rows in result without write lock • Read locks acquired when cursor is opened and held until transaction ends • Corresponds to table hints HOLDLOCK and SERIALIZABLE • Prevent dirty reads, non-repeatable reads, and phantom rows
Snapshot	<ul style="list-style-type: none"> • No read locks are applied • Read permitted on any row • Database snapshot of committed data is taken when the first row is read or updated by the transaction
Share mode (Default)	<ul style="list-style-type: none"> • Obtains a shared table lock on the table, preventing other transactions from modifying the table but allowing them read access. • If a transaction puts a shared lock on a table, it can change data in the table provided no other transaction holds a lock of any kind on the row(s) being modified.
Exclusive mode	<ul style="list-style-type: none"> • Obtains an exclusive table lock on the table, preventing other transactions from accessing the table. No other transaction can execute queries, updates, or any other action against the table.

6. Click **OK**.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Truncating Materialized View Data* on page 695

- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282

Truncating Materialized View Data

Truncate and refresh the materialized view to increase performance. Truncation cleans up stale materialized view data without deleting the view definition, and without removing any rows from the underlying table.

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the materialized view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • TRUNCATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • TRUNCATE permission on the materialized view. • You own the materialized view.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The materialized view is enabled.

Task

Materialized view data is read-only. Materialized views are only supported for system store (IQ catalog store) tables.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select one or more materialized views from the right pane and either:
 - Click the arrow to the right of the name and select **Truncate Data**, or
 - From the Administration Console menu bar, select **Resource > Truncate Data**.

Note: If the **Truncate Data** option is unavailable, refresh the data first.

Tip: Use **Shift-click** or **Control-click** to select multiple materialized views.

4. Click **Yes** to confirm truncation.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692
- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282

Validating Materialized View Data

Validate the data in an enabled materialized view.

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• You own the materialized view.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The materialized view is enabled.

Task

Materialized view data is read-only. Materialized views are only supported for system store (IQ catalog store) tables.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select one or more materialized views from the right pane and either:
 - Click the arrow to the right of the name and select **Validate Data**, or
 - From the Administration Console menu bar, select **Resource > Validate Data**.

Tip: Use **Shift-click** or **Control-click** to select multiple materialized views.

The **Validate Materialized Views** view appears. The Status column indicates the validation status of each materialized view listed.

4. Click **OK**.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282

Setting a Clustered Index

Using a clustered index increases the chance that two rows from adjacent index entries will appear on the same page in the database. This can lead to performance benefits by reducing the number of times a table page needs to be read into the buffer pool.

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the materialized view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The materialized view is enabled.
- At least one index for the materialized view exists.

Task

Materialized view data is read-only. Materialized views are only supported for system store (IQ catalog store) tables.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a single materialized view in the right pane, click the drop-down arrow that appears to the right, and select **Set Clustered Index**.
4. In the list of indexes, confirm the index you want to cluster. Clicking any index sets its **Clustered** value to **Yes** and changes all other **Clustered** values to **No**.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695

- *Validating Materialized View Data* on page 696
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Creating an Index on an IQ System Store Table* on page 589

Recompiling and Enabling a Materialized View

Recompile and enable a disabled materialized view to make it available for use by the database server.

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the materialized view and have one of the following: <ul style="list-style-type: none"> • SELECT permission on the underlying tables of the materialized view. • You own the underlying tables of the view.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view. <p>Also requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the underlying tables of the materialized view. • You own the underlying tables of the materialized view.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

- The materialized view is disabled.
- Recompile and enable any disabled materialized views referenced by this view.

Task

Materialized view data is read-only. Materialized views are only supported for system store (IQ catalog store) tables.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select one or more materialized views from the right pane and either:
 - Click the arrow to the right of the name and select **Recompile and Enable**, or
 - From the Administration Console menu bar, select **Resource > Recompile and Enable**.

Tip: Use **Shift-click** or **Control-click** to select multiple materialized views.

4. Click **Yes**.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695
- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282

Disabling a Materialized View

Disabling a materialized view makes it unusable, but retains the definition of the materialized view in the database. You can enable and recompile the disabled materialized view at a later time.

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the materialized view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The materialized view is enabled.
- In a multiplex configuration, the coordinator node is running.

Task

Materialized view data is read-only. Materialized views are only supported for system store (IQ catalog store) tables.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select one or more materialized views from the right pane and either:
 - Click the arrow to the right of the name and select **Disable**, or
 - From the Administration Console menu bar, select **Resource > Disable**.

Tip: Use **Shift-click** or **Control-click** to select multiple materialized views.

4. Click **Yes**.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691

- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695
- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Materialized View

Delete an enabled or disabled materialized view to remove it from the database. Deleting a materialized view deletes the definition of materialized view and its data, because a materialized view has its own physical storage (dbspace).

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• DROP ANY MATERIALIZED VIEW system privilege.• DROP ANY OBJECT system privilege.• You own the materialized view.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- In a multiplex configuration, the coordinator node is running.

Task

Materialized view data is read-only. Materialized views are only supported for system store (IQ catalog store) tables.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.

3. Select one or more materialized views from the right pane and either:

- Click the arrow to the right of the name and select **Delete**, or
- From the Administration Console menu bar, select **Resource > Delete**.

Note: Use **Shift-click** or **Control-click** to select multiple materialized views.

4. Click **Yes** to confirm deletion.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695
- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Materialized View DDL Commands

Display the data description language SQL code for adding a materialized view to the database. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

Materialized view data is read-only. Materialized views are only supported for system store (IQ catalog store) tables.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select one or more materialized views from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple materialized views.

The DDL view shows the SQL code used to add the selected materialized views to the database.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695
- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Materialized View Properties

View or change materialized view properties including the SQL view definition (including the column definition), the amount of free space you want to reserve for each materialized view page, permissions on the materialized view, and the refresh type.

Prerequisites

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any materialized view property page – None required.</p> <p>Modify materialized view permissions – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object. <p>Modify the SQL page of the materialized view properties – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the materialized view and have SELECT permission on the underlying tables. <p>Modify any other materialized view property except those relating to indexes – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying tables. • SELECT permission on the underlying tables. • You own the materialized view. <p>For privileges relating to materialized view indexes, see:</p> <ul style="list-style-type: none"> • <i>Materialized View Index Privilege Summary</i> on page 743

Database Version	Materialized View Privileges
SAP Sybase IQ 16.0	<p>View any materialized view property page – None required.</p> <p>Modify materialized view permissions – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object. <p>Modify a materialized view comment – Requires any one of:</p> <ul style="list-style-type: none"> • CREATE ANY MATERIALIZED VIEW system privilege • ALTER ANY MATERIALIZED VIEW system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege • You own the materialized view. <p>Modify the SQL page of the materialized view properties – Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY MATERIALIZED VIEW system privilege. • DROP ANY OBJECT system privilege. • You own the materialized view. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY MATERIALIZED VIEW system privilege. • CREATE ANY OBJECT system privilege. <p>Modify any other materialized view property except those relating to indexes – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view. <p>For privileges relating to materialized view indexes, see:</p> <ul style="list-style-type: none"> • <i>Materialized View Index Privilege Summary</i> on page 743

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

Materialized view data is read-only. Materialized views are only supported for system store (IQ catalog store) tables.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

Note:

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.
-
4. View or modify the properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) Name of the materialized view.</p> <p>Owner – (Read-only) Owner of the materialized view.</p> <p>DbSPACE – (Read-only) Name of the dbSPACE the materialized view created on.</p> <p>Database – (Read-only) Name of the database the materialized view is created in.</p> <p>Status – Status of materialized view. Valid statuses are Enabled and Disabled.</p> <ul style="list-style-type: none"> • Recompile and Enable – Select to recompile the materialized view. • Disable – Select to disable the materialized view. <p>Optimized – Select to enable optimization.</p> <p>Initialized – Initialized status of materialized view. Valid statuses are Yes and No.</p> <ul style="list-style-type: none"> • Refresh – Select to refresh the current materialized view. • Truncate – Select to truncate the materialized view. <p>Refresh type – (Read-only) Refresh method defined for the materialized view.</p> <p>Immediate compatible – (Read-only) Immediate compatible status of materialized view.</p> <p>Last refresh time – (Read-only) Date and time last refresh performed</p> <p>Known stale time – (Read-only) Length of time between refreshes.</p> <p>Comment – A text field for adding an optional comment about the materialized view.</p>
SQL	The SELECT statement used to create the materialized view.
Columns (Read-only)	<p>Name – Column name.</p> <p>ID – Column ID.</p> <p>Data Type – Column Data type.</p> <p>Allows null – Indicates if the column accepts null values. Either Yes or No.</p>

Area	Description
Data	<div> Note: <ul style="list-style-type: none"> For 15.3 and 15.4, requires SELECT permission on the underlying table to view data. For 16.0, requires the SELECT ANY TABLE system privilege to view data. </div> <hr/> Displays the first 500 rows of data.
Permissions	See <i>Materialized View Permissions</i> on page 719.
Referenced Objects (Read-only)	Name – Table name. Owner – Table owner. Object Type – Referenced object type (Table, for example). Referenced Column – Column ID. Dependency Type – Indicates Direct or Indirect dependency.
Dependent Views (Read-only)	Name – View name. Owner – View owner. View Type – View type. Dependency Type – Indicates Direct or Indirect dependency.
Indexes	See <i>Materialized View Indexes</i> on page 733.

Area	Description
Options (Read-only)	<p>date_format – Sets the format for dates retrieved from the database. The default is YYYY-MM-DD.</p> <p>date_order – Controls the interpretation of date formats. The default is YMD. For Open Client and jConnect connections, the default is set to MDY.</p> <p>default_timestamp_increment – Specifies the number of microseconds to add to a column of type <code>TIMESTAMP</code> to keep values in the column unique. The default is 1.</p> <p>first_day_of_week – Sets the numbering of the days of the week. The default is 7 (Sunday is the first day of the week).</p> <p>nearest_century – Controls the interpretation of two-digit years in string-to-date conversions. The default is 50.</p> <p>precision – Specifies the maximum number of digits in the result of any decimal arithmetic. The default is 30.</p> <p>scale – Specifies the minimum number of digits after the decimal point when an arithmetic result is truncated to the maximum precision. The default is 6.</p> <p>time_format – Sets the format for times retrieved from the database. The default is HH:NN:SS.SSS.</p> <p>timestamp_format – Sets the format for timestamps that are retrieved from the database. The default is YYYY-MM-DD HH:NN:SS.SSS.</p> <p>timestamp_with_timezone_format – Sets the format for timestamps that are retrieved from the database. The default is YYYY-MM-DD HH:NN:SS.SSS+HH:NN.</p> <p>uuid_has_hyphens – Controls the formatting of unique identifier values when they are converted to strings. Valid values are On (default) and Off.</p>

Area	Description
Miscellaneous	<p>Number of rows: (approximate) – Approximate number of rows in the view. To update this value, click Calculate.</p> <p>Calculate – Calculates the number of rows in the view.</p> <p>Default – Choose this option to reserve 200 bytes in each page.</p> <p>Percentage – Choose this option to specify an integer between 0 and 100. The former specifies that no free space is to be left on each page—each page is to be fully packed. A high value causes each row to be inserted into a page by itself.</p> <p>Materialized view data is encrypted – When the database is created with table encryption scope, you can select this option to encrypt this materialized view's data.</p>

5. Click **OK**.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695
- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733
- *Authenticating a Login Account for a Managed Resource* on page 282

Materialized View Privilege Summary

A list of the system privileges and object permissions required to complete the various materialized view tasks.

Creating a Materialized View

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Materialized view to be owned by self –</p> <ul style="list-style-type: none"> • Requires RESOURCE authority with SELECT permission on tables in the view definition. • Requires CREATE permission on the selected dbspace to create a view owned by you. <p>Materialized view to be owned by any user – Requires DBA authority.</p>
SAP Sybase IQ 16.0	<p>Materialized view to be owned by self –</p> <ul style="list-style-type: none"> • Requires CREATE MATERIALIZED VIEW system privilege. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE object permission on the dbspace where the materialized view is being created. • Also requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT object permission on the underlying tables of the materialized view. <p>Materialized view to be owned by any user –</p> <ul style="list-style-type: none"> • Requires CREATE object permission on the dbspace where the materialized view is being created. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY MATERIALIZED VIEW system privilege. • CREATE ANY OBJECT system privilege. • And also requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT object permission on the underlying tables of the materialized view.

Viewing Materialized View Data in the Execute SQL Window

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	None required. Query executes with user's current permissions.
SAP Sybase IQ 16.0	None required. Query executes with user's current permissions.

Truncating Materialized View Data

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the materialized view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • TRUNCATE ANY TABLE system privilege. • ALTER ANY TABLE system privilege. • ALTER ANY OBJECT system privilege. • TRUNCATE permission on the materialized view. • You own the materialized view.

Validating Materialized View Data

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the materialized view.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

Refreshing Materialized View Data

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires DBA authority.</p> <p>Also requires both of:</p> <ul style="list-style-type: none"> • INSERT permission on the underlying tables of the materialized view or you own the materialized view. • SELECT permission on the underlying tables of the materialized view or you own the underlying tables of the materialized view.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • INSERT ANY TABLE system privilege. • INSERT permission on the materialized view. • You own the materialized view. <p>Also requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the underlying tables of the materialized view. • You own the underlying tables of the materialized view.

Recompiling and Enabling Materialized View Data

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the materialized view and have one of the following: <ul style="list-style-type: none"> • SELECT permission on the underlying tables of the materialized view. • You own the underlying tables of the view.

Database Version	Materialized View Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view. <p>Also requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the underlying tables of the materialized view. • You own the underlying tables of the materialized view.

Disabling Materialized View Data

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the materialized view.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view.

Deleting a Materialized View

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY MATERIALIZED VIEW system privilege. • DROP ANY OBJECT system privilege. • You own the materialized view.

Generating Materialized View DDL Commands

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Setting a Clustered Index on a Materialized View

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the materialized view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view.

Viewing or Modifying Materialized View Properties

Database Version	Materialized View Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any materialized view property page – None required.</p> <p>Modify materialized view permissions – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object. <p>Modify the SQL page of the materialized view properties – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the materialized view and have SELECT permission on the underlying tables. <p>Modify any other materialized view property except those relating to indexes – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the underlying tables. • SELECT permission on the underlying tables. • You own the materialized view. <p>For privileges relating to materialized view indexes, see:</p> <ul style="list-style-type: none"> • <i>Materialized View Index Privilege Summary</i> on page 743

Database Version	Materialized View Privileges
SAP Sybase IQ 16.0	<p>View any materialized view property page – None required.</p> <p>Modify materialized view permissions – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object. <p>Modify a materialized view comment – Requires any one of:</p> <ul style="list-style-type: none"> • CREATE ANY MATERIALIZED VIEW system privilege • ALTER ANY MATERIALIZED VIEW system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege • You own the materialized view. <p>Modify the SQL page of the materialized view properties – Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY MATERIALIZED VIEW system privilege. • DROP ANY OBJECT system privilege. • You own the materialized view. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY MATERIALIZED VIEW system privilege. • CREATE ANY OBJECT system privilege. <p>Modify any other materialized view property except those relating to indexes – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY MATERIALIZED VIEW system privilege. • ALTER ANY OBJECT system privilege. • You own the materialized view. <p>For privileges relating to materialized view indexes, see:</p> <ul style="list-style-type: none"> • <i>Materialized View Index Privilege Summary</i> on page 743

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695

- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Permissions* on page 719
- *Materialized View Indexes* on page 733

Materialized View Permissions

Grant or revoke materialized view permissions to users and roles.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695
- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Indexes* on page 733

About the Materialized View Permissions List

The materialized view permissions list displays details on the specific object permissions directly granted to users or roles for a single view.

There are four object permissions for views or materialized views, which can be granted with or without administrative rights:

- SELECT
- INSERT
- DELETE
- UPDATE

These object permissions can be granted in several ways:

- You own the object.
- You are granted the **MANAGE ANY OBJECT PRIVILEGE** system privilege.
- You have been indirectly granted specific permissions through membership in a role to which permissions have been directly or indirectly granted.
- You have been directly granted specific permissions.

Users or roles with object ownership or the **MANAGE ANY OBJECT PRIVILEGE** system privilege are automatically granted all possible object permissions with administrative rights.

The permissions list only lists those permissions granted directly to user or roles. The list indicates who the permissions are granted to whom (grantee), by who (grantor), and the permissions and their corresponding administrative rights. The permissions list does not list object permissions obtained through ownership, the **MANAGE ANY SYSTEM OBJECT** system privilege, or role membership.

The permissions list only lists those permissions granted directly to user or roles. The list indicates who the permissions are granted to whom (grantee), by who (grantor), and the permissions and their corresponding administrative rights. The permissions list does not list object permissions obtained through ownership, the **MANAGE ANY SYSTEM OBJECT** system privilege, or role membership.

Grantee	grantor	Select	Insert	Delete	Update
Manager1	Manager1	✓ ↔	✓ ↔	✓ ↔	✓ ↔
User2	Manager1	✓		✓	
User2	User1		✓ ↔		

Legend:
✓ Permission granted with no administrative rights
✓ ↔ Permission granted with administrative rights

When granted to a role, permissions, including administrative rights, are inherited by all members of the role. The role, not the users indirectly granted the permissions through inheritance, appear on the permissions list.

The **REVOKE** command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the **SELECT** permission with the **With grant option**. UserA grants **SELECT** to UserB with the **With grant option**. UserB grants **SELECT** to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the **SELECT** permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

Permissions can be granted on the same view or materialized view, to the same grantee, by multiple grantors, resulting in the same grantee appearing multiple times on the list. If the same permission is granted to the same grantee, with and without administrative rights, the grant with the administrative right takes precedence.

Grantee	grantor	Select	Insert	Delete	Update
Manager1	Manager1	✓ ↔	✓ ↔	✓ ↔	✓ ↔
User2	Manager1	✓	✓	✓	
User2	User1		✓ ↔		



When revoking a permission granted multiple times, the permission is revoked from all instances, regardless of administrative rights. For example, Manager1 grants User2 **INSERT** with administrative rights. User1 also grants **INSERT** to User2, but without administrative rights. Regardless of which instance of **INSERT** is revoked, both instances of **INSERT** are revoked for User2.

Following the Materialized View Permission Trail

Before revoking a grantee's permission, you need to identify grantees directly or indirectly granted the permission from the original grantee.

The grant chain traces how a grantee has in turn granted a permission to other grantees.

Consider the following:

- Bob is granted all permissions with administrative rights.
- Bob grants Joe **SELECT** permission without administrative rights. Bob also grants Jane **SELECT** and **INSERT** permissions with administrative rights.
- Jane grants Mike and Joe **SELECT** and **DELETE** permissions with administrative rights. Jane also grants Beth and Mary **SELECT** permissions without administrative rights.

Note: Joe has now been granted the **SELECT** permission twice, with different administrative rights, by different grantors.

- Joe grants Beth **SELECT** permission without administrative rights

Note: Beth has now been granted the **SELECT** permission twice, by different grantors.

- Mike grants Sarah SELECT and UPDATE permission with administrative rights. Mike also grants Alice SELECT permission without administrative rights.
- Sarah grants Alex, Beth, and Role1 SELECT and UPDATE permissions without administrative rights.

Note: Beth has now been granted the SELECT permission multiple times, by different grantors.

The permissions list would appear similar to:

Permissions

Grant...

Revoke

Grantee	1 ▲	grantor	Select	Insert	Delete	Update
Alex		Sarah	✓			✓
Alice		Mike	✓			
Beth		Jane	✓			
Beth		Joe	✓			
Beth		Sarah	✓			✓
Bob		Manager	✓ ↔	✓ ↔	✓ ↔	✓ ↔
Jane		Bob	✓ ↔	✓ ↔		
Joe		Bob	✓			
Joe		Jane	✓ ↔		✓ ↔	
Mary		Jane	✓			
Mike		Jane	✓ ↔		✓ ↔	
Role1		Sarah	✓			✓
Sarah		Mike	✓ ↔			✓ ↔

You want to revoke **SELECT** permission from Jane. To determine the potential impact on other users and roles, do the following:

Tip: For complex grant trails, create a tree diagram to visually track the grant chain.

1. Sort the list by Grantor and locate all instances of administrative grants of SELECT by Jane.

Permissions					
			Grant... Revoke		
Grantee	1 grantor 1 ▲	Select	Insert	Delete	Update
Jane	Bob	✓ ↔	✓ ↔		
Joe	Bob	✓			
Mike	Jane	✓ ↔		✓ ↔	
Joe	Jane	✓ ↔		✓ ↔	
Beth	Jane	✓			
Mary	Jane	✓			
Beth	Joe	✓			
Bob	Manager	✓ ↔	✓ ↔	✓ ↔	✓ ↔
Alice	Mike	✓			
Sarah	Mike	✓ ↔			✓ ↔
Beth	Sarah	✓			✓
Alex	Sarah	✓			✓
Role1	Sarah	✓			✓

Note: There are four instances of Jane granting permissions. Since we are revoking the SELECT permission only, only those grants involving the SELECT permission will be impacted. Therefore, revoking Jane's SELECT permission will also revoke the permission from Mary, Mike, and Beth. Of the SELECT permissions, we need to follow those involving administrative rights.

2. Locate Mike in the Grantor column.

						Grant...	Revoke
Grantee	grantor	1 ▲	Select	Insert	Delete	Update	
Jane	Bob		✓ ↔	✓ ↔			
Joe	Bob		✓				
Mike	Jane		✓ ↔		✓ ↔		
Joe	Jane		✓ ↔		✓ ↔		
Beth	Jane		✓				
Mary	Jane		✓				
Beth	Joe		✓				
Bob	Manager		✓ ↔	✓ ↔	✓ ↔	✓ ↔	
Alice	Mike		✓				
Sarah	Mike	2	✓ ↔			✓ ↔	
Beth	Sarah		✓			✓	
Alex	Sarah		✓			✓	
Role1	Sarah		✓			✓	

Note: Mike granted SELECT to Sarah and Alice. Both were granted the SELECT permission as an indirect (once removed) result of Jane. It does not matter whether the grant included administrative rights. Therefore, their SELECT permission will also be revoked when Jane's is revoked. Since Alice was granted SELECT without administrative rights, her grant chain ends. Since Sarah was granted SELECT with administrative rights, her grant chain continues.

3. Locate Sarah in the Grantor column.

Permissions						
<div>Grant...</div> <div>Revoke</div>						
Grantee	grantor	1 ▲	Select	Insert	Delete	Update
Jane	Bob		✓ ↔	✓ ↔		
Joe	Bob		✓			
Mike	Jane		✓ ↔		✓ ↔	
Joe	Jane		✓ ↔		✓ ↔	
Beth	Jane		✓			
Mary	Jane		✓			
Beth	Joe		✓			
Bob	Manager		✓ ↔	✓ ↔	✓ ↔	✓ ↔
Alice	Mike		✓			
Sarah	Mike		✓ ↔			✓ ↔
Beth	Sarah		✓			✓
Alex	Sarah 3		✓			✓
Role1	Sarah		✓			✓

Note: Sarah granted SELECT to Beth and Alex. Both were granted the SELECT permission as an indirect (twice removed) result of Jane. Again, administrative rights do not matter, and since neither grant was with administrative rights, the grant chain ends.

To summarize, revoking Jane's SELECT permission revokes the permission from Mike, Joe, Beth, and Mary, through direct granting or permissions by Jane, but also revokes the permission from Alice, Sarah, Alex, and Role1 as a result of indirect from Jane. The permissions list after revoking Jane's SELECT permission would appear similar to:

							Grant...	Revoke
Grantee	grantor	1 ▲	Select	Insert	Delete	Update		
Jane	Bob		✓ ↔	✓ ↔				
Joe	Bob		✓					
Mike	Jane		✓ ↔		✓ ↔			
Joe	Jane		✓ ↔		✓ ↔			
Beth	Jane		✓					
Mary	Jane		✓					
Beth	Joe		✓					
Bob	Manager		✓ ↔	✓ ↔	✓ ↔	✓ ↔		
Alice	Mike		✓					
Sarah	Mike		✓ ↔			✓ ↔		
Beth	Sarah		✓			✓		
Alex	Sarah		✓			✓		
Role1	Sarah		✓			✓		

It is important to note that it is possible for a user to retain an "identified" permission after revoke it the same permission was granted by multiple grantors. In this scenario, both Bob and Jane granted the SELECT permission to Joe, so Joe retains the SELECT permission granted by Bob. If a grantee has been granted multiple permissions, only those permissions explicitly selected are revoked. In this scenario, only the SELECT permission was revoked from Joe. The DELETE permission remains granted, even though it was also granted by Jane.

							Grant...	Revoke
Grantee	grantor		Select	Insert	Delete	Update		
Alex	Sarah					✓		
Beth	Sarah					✓		
Bob	Manager		✓ ↔	✓ ↔	✓ ↔	✓ ↔		
Jane	Bob			✓ ↔				
Joe	Bob		✓					
Joe	Jane				✓ ↔			
Mike	Jane				✓ ↔			
Role1	Sarah					✓		
Sarah	Mike					✓ ↔		

Granting Materialized View Permissions

Grant materialized view permissions to users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object.
SAP Sybase IQ	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
6. On the Welcome page, indicate whether the permission is being granted to a user or role.
7. Click **Next**.

8. On the Grantees page, select one or more users or roles. Click the box in the header row to select all available users or roles.
9. Click **Next**.
10. On the Permissions page, select one or more permissions. Click the box in the header row to select all available permissions.
11. Click **Next**.
12. (Optional) Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

13. Click **Finish**.

14. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Revoking Materialized View Permissions

Remove materialized view permissions from users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• Administrative rights over the permission.• You own the database object.
SAP Sybase IQ	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You have administrative rights (with grant option) to the permission.• You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right

only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the **SELECT** permission with the **With grant option**. UserA grants **SELECT** to UserB with the **With grant option**. UserB grants **SELECT** to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the **SELECT** permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, select a user or role granted permissions to be revoked, and click **Revoke**.
A list of permissions currently granted (regardless of administrative rights) appears..
6. Select one or more permissions to revoke. Click the box in the header row to select all available permissions.

Warning! Revoking permissions may result in unexpected revocation from other users or groups. See *Following the Materialized View Permission Grant Trail*.

7. Click **Finish**.
8. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Removing Administrative Rights Only from a Materialized View Permission

Remove administrative rights only from a granted materialized view permission.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are logged on as the original grantor of the permission with administrative rights to be removed.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, click **Grant**.
6. On the Welcome page, indicate whether the grantee is a user or role.
7. Click **Next**.
8. On the Grantees page, select the grantee..
9. Click **Next**.
10. On the Permissions page, select the permissions from which the administrative rights are being revoked.
11. Click **Finish**.
12. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Adding Administrative Rights to a Granted Materialized View Permission

Add administrative rights only to a granted materialized view permission.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the Administration Console, expand **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, select the grantee to have administrative rights granted on a permission. If the grantee appears on the list multiple times with the same permission granted, it does not matter which instance is selected.
6. In the right pane, click **Grant**.
7. On the Welcome page, indicate whether the grantee is a user or role.
8. Click **Next**.
9. On the Grantees page, select the grantee..
10. Click **Next**.
11. On the Permissions page, select the permission to which administrative rights are to be granted.
12. Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

13. Click **Finish**.
14. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Materialized View Permissions Privilege Summary

A list of the system privileges and object permissions required to complete the various materialized view permission tasks.

Grant and Revoke Permissions on a Materialized View

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object.
SAP Sybase IQ	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

Adjust Administration Permissions on a Materialized View

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

Materialized View Indexes

You can add multiple indexes to any column in the materialized view to better support the queries you plan to run.

It is more efficient to create all the indexes needed before you insert any data into your database. You can drop any of the optional indexes later if you decide you do not need them.

Indexes can greatly improve the performance of searches on the indexed columns. However, indexes take up space within the database and slow down insert, update, and delete operations. This section helps you determine when you should create an index and how to achieve maximum performance from your index.

There are many situations in which creating an index improves the performance of a database. An index provides an ordering of a table's rows based on the values in some or all of the columns. An index allows the database server to find rows quickly. It permits greater concurrency by limiting the number of database pages accessed. An index also affords the database server a convenient means of enforcing a uniqueness constraint on the rows in a table.

See also

- *Creating a Materialized View* on page 689
- *Viewing Materialized View Data in the Execute SQL Window* on page 691
- *Refreshing Materialized View Data* on page 692
- *Truncating Materialized View Data* on page 695
- *Validating Materialized View Data* on page 696
- *Setting a Clustered Index* on page 698
- *Recompiling and Enabling a Materialized View* on page 699
- *Disabling a Materialized View* on page 701
- *Deleting a Materialized View* on page 702
- *Generating Materialized View DDL Commands* on page 703
- *Viewing or Modifying Materialized View Properties* on page 705
- *Materialized View Privilege Summary* on page 712
- *Materialized View Permissions* on page 719

Creating a Materialized View Index

Create an index on a materialized view.

Prerequisites

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority• You own the underlying database object of the index.

Database Version	Materialized View Index Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace, along with one of: <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • You own the materialized view index.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

Indexes improve search performance on the indexed column or columns. Indexes take up space in the database, however, and slow down the performance of insert, delete, and update operations.

When creating indexes, the order in which you specify the columns becomes the order in which the columns appear in the index. Duplicate references to column names in the index definition are not allowed.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

4. In the left pane, select **Indexes**.
5. Click **New**.
6. On the Index Name page, specify a name for the index.
7. Click **Next**.
8. On the Columns page, highlight one or more columns and click **Add Asc** or **Add Desc**

Note: Use **Shift-click** or **Control-click** to select multiple columns.

- a) In the **Columns in index** list, highlight a single column and click the up and down buttons to reposition the column.
 - b) Highlight one or more columns and click **Remove** to remove columns from the index.
9. Click **Next**.
 10. On the Uniqueness page, indicate if the index is unique.

11. Click Next.

12. On the Index Clustering page, indicate if the index is clustered and the dbspace to store the index.

13. Click Next.

14. (Optional) On the Comment page, enter a text comment for the index.

15. Click Finish.

The index appears in the properties view, but is not saved to the database.

16. Do one of the following:

- Click **Apply** to upload any property changes to the database and remain in the properties view.
- Click **OK** to upload any property changes to the database and exit the properties view.
- Click **Cancel** to cancel any unsaved property changes and exit the properties view.

See also

- *Creating a Materialized View Index* on page 734
- *Column Index Types* on page 587

Deleting a Materialized View Index

Unused indexes take up space in your database. Delete a materialized view index if you do not require it.

Prerequisites

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• RESOURCE authority with ALTER permission on the underlying database object of the index.• You own the underlying database object of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• DROP ANY INDEX system privilege.• DROP ANY OBJECT system privilege.• You own the materialized index.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

4. In the left pane, select **Indexes**.
5. Select one or more indexes from the right pane.

Note: Use **Shift-click** or **Control-click** to select multiple indexes.

6. Click **Delete**.

Warning! There is no confirmation prompt before the indexes are deleted

7. Do one of the following:

- Click **Apply** to upload any property changes to the database and remain in the properties view.
- Click **OK** to upload any property changes to the database and exit the properties view.
- Click **Cancel** to cancel any unsaved property changes and exit the properties view.

Rebuilding a Materialized View Index

As data is modified in the underlying tables that the indexes operate on, the indexes become fragmented. Rebuild fragmented indexes on materialized views to improve performance.

Prerequisites

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the underlying database object of the index. • You own the underlying database object of the index.

Database Version	Materialized View Index Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • You own the underlying database object of the index.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

4. In the left pane, select **Indexes**.
5. Select one or more indexes from the right pane and click **Rebuild**.

Note: Use **Shift-click** or **Control-click** to select multiple indexes.

The Rebuild Indexes view appears when complete and indicates the rebuild status of each selected index.

6. Click **OK**.

Validating a Materialized View Index

Validate an index on a materialized view.

Prerequisites

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • VALIDATE authority.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

4. In the left pane, select **Indexes**.
5. Select one or more indexes from the right pane and click **Validate**.

Note: Use **Shift-click** or **Control-click** to select multiple indexes.

Note: **Validate** does not appear when the underlying table is an IQ store (main store) table.

The Validate Indexes view appears when complete and indicates the validation status of each selected index.

6. Click **OK**.

Generating Materialized View Index DDL Commands

Display the data description language SQL code for adding an index to a materialized view. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

4. In the left pane, select **Indexes**.
5. Select one or more indexes from the right pane and click **Generate DDL**.

Note: Use **Shift-click** or **Control-click** to select multiple indexes.

6. Click **Generate DDL**.

The DDL window shows the SQL code used to add the selected index to the table or materialized view.

Viewing or Modifying Materialized View Index Properties

Display and edit the properties for the selected materialized view index.

Prerequisites

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any materialized view index property page – None required.</p> <p>Modify any materialized view index property – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• RESOURCE authority with ALTER permission on the underlying database object of the index.• You own the underlying database object of the index.

Database Version	Materialized View Index Privileges
SAP Sybase IQ 16.0	<p>View any materialized view index property page – None required.</p> <p>Modify a materialized view index comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • ALTER ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. <hr/> <p>Note: ALTER permission on the materialized view is not required to modify the comment only.</p> <hr/> <p>Modify any other materialized view index property – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace, along with one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • You own the materialized view.

- The SAP Sybase IQ resource is authenticated and running.
- (Modifying properties only) In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Views > Materialized Views**.
3. Select a materialized view from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Materialized View Properties view appears.

4. In the left pane, select **Indexes**.
5. Click **Edit**.
The Indexes Properties view appears.
6. View or modify the properties.
 - Any modifications to the properties are saved when either **Apply** or **OK** is clicked
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – Name of the index.</p> <p>Unique – (Read-only) Whether values in the index must be unique. The unique value is set when you create a new index.</p> <p>Table – (Read-only) Name and owner of the table with which the index is associated.</p> <p>Dbospace – (Read-only) Database file, or dbospace, where the index is located.</p> <p>Index Type – (Read-only) Index type (High Non-Group, for example).</p> <p>Clustered – (Read-only) Whether this is a clustered index. Clustered indexes store the table rows in approximately the same order as they appear in the corresponding index. Using a clustered index can lead to performance benefits by reducing the number of times each page needs to be read into memory. Only one index on a table can be a clustered index.</p> <p>Format – (Read-only) The store type of the index.</p> <p>Comment – User-defined text description of the index. For example, the index's purpose in the system.</p>
Columns (Read-only)	<p>Name – Name of the columns indexed.</p> <p>Sequence – Columns are sorted by their sequence, which is a unique number starting at 0. The order of the numbers determines the relative position of the columns in the index.</p> <p>Order – Either ascending or descending order. Set the order when you create a new index.</p> <p>Data Type – Data type of the columns indexed.</p>
Placement (Read-only)	<p>Dbospace – Dbospace occupied by the object.</p> <p>Size – Size of the object.</p> <p>% File – Percentage of the file used by this object.</p> <p>First Block – First block used by this object.</p> <p>Last Block – Last block used by this object.</p>

Area	Description
Fragmentation (Read-only)	<p>Fill Percent – Range of how full pages are, for example, between 11 and 20% full. All percentages are truncated to the nearest percentage point.</p> <p>BTree Pages – Number of B-tree pages in the index with a particular fill percent.</p> <p>GArray Pages – Number of GArray pages in the index with a particular fill percent.</p> <p>Bitmap Pages – Number of bitmap pages in the index with a particular fill percent.</p>

7. Click **OK**.

Index property modifications are not yet saved to the database.

8. Do one of the following:

- Click **Apply** to upload any property changes to the database and remain in the properties view.
- Click **OK** to upload any property changes to the database and exit the properties view.
- Click **Cancel** to cancel ALL unuploaded property changes and exit the properties view.

Materialized View Index Privilege Summary

A list of the system privileges and object permissions required to complete the various index tasks materialized views.

Creating a Materialized View Index

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority • You own the underlying database object of the index.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the dbspace, along with one of: <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • You own the materialized view index.

Deleting a Materialized View Index

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the underlying database object of the index. • You own the underlying database object of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY INDEX system privilege. • DROP ANY OBJECT system privilege. • You own the materialized index.

Rebuilding a Materialized View Index

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the underlying database object of the index. • You own the underlying database object of the index.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • You own the underlying database object of the index.

Validating a Materialized View Index

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • VALIDATE authority.
SAP Sybase IQ 16.0	Requires VALIDATE ANY OBJECT system privilege.

Generating Materialized View Index DDL Commands

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Materialized View Index Properties

Database Version	Materialized View Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any materialized view index property page – None required.</p> <p>Modify any materialized view index property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority with ALTER permission on the underlying database object of the index. • You own the underlying database object of the index.
SAP Sybase IQ 16.0	<p>View any materialized view index property page – None required.</p> <p>Modify a materialized view index comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege. • ALTER ANY INDEX system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. <hr/> <p>Note: ALTER permission on the materialized view is not required to modify the comment only.</p> <hr/> <p>Modify any other materialized view index property – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY OBJECT system privilege. • CREATE permission on the dbspace, along with one of: <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • You own the materialized view.

Domains

Domains are user-defined data types. They improve convenience and encourage consistency in the database.

Domains allow you to define columns on the same data type automatically throughout a database. Domains can have the same NULL or NOT NULL condition, with the same DEFAULT setting and the same CHECK condition.

Creating a Domain

Use the Create Domain wizard to create an SAP Sybase IQ domain.

Prerequisites

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• RESOURCE authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• CREATE DATATYPE system privilege.• CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Domains**.
3. Click the arrow next to **Domain** and select **New**.
The Create Domain Wizard appears.
4. On the Welcome page, specify

Option	Description
Select a resource for which the domain will be created	From the list, select the resource for which the domain will be created.
What do you want to name the domain?	Enter a unique name for the new domain; maximum of 128 characters.
Which built-in type do you want to use?	<p>From the list, select the domain type. Specify the size, scale and unit when enabled for specify types.</p> <p>Note: For appropriate data type options and default values, in the <i>SAP Sybase IQ</i> documentation, see <i>Reference: Building Blocks, Tables, and Procedures > SQL Data Types</i>.</p>

5. Click **Next**.
6. On the Clauses page, specify

Option	Description
This domain has a default value	Select to define a default value.
Null values	Select whether null values will be allowed. Default is to use the database default setting, which allows null values.

7. Click **Next**.
8. On the Check Constraint page, specify a check constraint for the domain.
9. Click **Finish**.

See also

- *Deleting a Domain* on page 751
- *Generating Domain DDL Commands* on page 752
- *Viewing Domain Properties* on page 753
- *Domain Privilege Summary* on page 754
- *Authenticating a Login Account for a Managed Resource* on page 282

Constraints and Defaults with Domains

Many of the attributes associated with columns, such as allowing NULL values, having a DEFAULT value, and so on, can be built into a user-defined data type.

Any column that is defined on the data type automatically inherits the NULL setting, CHECK condition, and DEFAULT values. This allows uniformity to be built into columns with a similar meaning throughout a database.

For example, many primary key columns in the demo database are integer columns holding ID numbers. The following statement creates a data type that may be useful for such columns:

```
CREATE DOMAIN id INT
NOT NULL
DEFAULT AUTOINCREMENT
CHECK ( @col > 0 )
```

Any column created using the data type `id` is not allowed to hold NULLs, defaults to an autoincremented value, and must hold a positive number. Any identifier could be used instead of `col` in the `@col` variable.

The attributes of the data type can be overridden if needed by explicitly providing attributes for the column. A column created on data type `id` with NULL values explicitly allowed does allow NULLs, regardless of the setting in the `id` data type.

See also

- *Compatibility Considerations for Domains* on page 748

Compatibility Considerations for Domains

Ensure compatibility with SQL Anywhere and Adaptive Server Enterprise when you create domains.

NULL in Columns

For compatible treatment of NULL:

- SQL Anywhere and SAP Sybase IQ assume that columns can be null unless NOT NULL is stated in the column definition. You can change this behavior by setting the database option **ALLOW_NULLS_BY_DEFAULT** to the Transact-SQL compatible setting OFF.
- SQL Anywhere and SAP Sybase IQ assume that BIT columns cannot be NULL.
- Adaptive Server Enterprise assumes that columns cannot be null unless NULL is stated.

Check Constraints

SAP Sybase IQ enforces check constraints on base, global temporary, and local temporary tables, and on user-defined data types. Users can log check integrity constraint violations and specify the number of violations that can occur before a **LOAD** statement rolls back.

SAP Sybase IQ does not allow the creation of a check constraint that it cannot evaluate, such as those composed of user-defined functions, proxy tables, or non-SAP Sybase IQ tables.

Constraints that cannot be evaluated are detected the first time the table on which the check constraint is defined is used in a **LOAD**, **INSERT**, or **UPDATE** statement. SAP Sybase IQ does not allow check constraints containing:

- Subqueries
- Expressions specifying a host language parameter, a SQL parameter, or a column as the target for a data value
- Set functions

- Invocations of nondeterministic functions or functions that modify data

Adaptive Server Enterprise and SQL Anywhere enforce **CHECK** constraints. SQL Anywhere allows subqueries in check constraints.

SAP Sybase IQ supports user-defined data types that allow constraints to be encapsulated in the data type definition.

Referential Integrity Constraints

Actions for enforcing integrity are supported as follows:

- SAP Sybase IQ supports all ANSI actions: SET NULL, CASCADE, DEFAULT, RESTRICT.
- Adaptive Server Enterprise supports two of these actions: SET NULL, DEFAULT.

Note: You can achieve CASCADE in Adaptive Server Enterprise by using triggers instead of referential integrity.

- SAP Sybase IQ supports the RESTRICT action only.
- SAP Sybase IQ does not support NOT NULL FOREIGN KEY.
- SAP Sybase IQ has the restriction that a column cannot be both a candidate key and a foreign key at the same time.

Default Values in a Column

Default value support differs as follows:

- Adaptive Server Enterprise and SQL Anywhere support specifying a default value for a column.
- Only SQL Anywhere supports DEFAULT UTC TIMESTAMP.
- SAP Sybase IQ supports specifying a default value for a column, except for the special values DEFAULT UTC TIMESTAMP and DEFAULT CURRENT UTC TIMESTAMP. SAP Sybase IQ also ignores settings for the DEFAULT_TIMESTAMP_INCREMENT database option.

Identity Columns

Identity column support differs as follows:

- SAP Sybase IQ supports IDENTITY or DEFAULT AUTOINCREMENT as a default value. SAP Sybase IQ supports identity columns of any numeric type with any precision and scale 0, and the column can be NULL. SAP Sybase IQ identity columns must be positive and are limited by the range of the data type. SAP Sybase IQ supports a single identity column per table, and requires database option IDENTITY_INSERT set to a table name for explicit inserts and updates. To drop a table with an IDENTITY column, you cannot have IDENTITY_INSERT set to that table. The table can contain data when adding an identity column. Tables derived using SELECT INTO do not have Identity/

Autoincrement columns. SAP Sybase IQ views cannot contain `IDENTITY/DEFAULT` `AUTOINCREMENT` columns.

- SQL Anywhere supports the `AUTOINCREMENT` default value. SQL Anywhere supports identity columns of any numeric type with any allowable scale and precision. The identity column value can be positive, negative, or zero, limited by the range of the data type. SQL Anywhere supports any number of identity columns per table, and does not require `identity_insert` for explicit inserts, drops, and updates. The table must be empty when adding identity columns. SQL Anywhere identity columns can be altered to be nonidentity columns, and vice versa. You can add or drop `AUTOINCREMENT` columns from SQL Anywhere views.
- Adaptive Server Enterprise supports a single identity column per table. Adaptive Server Enterprise identity columns are restricted to only numeric data type scale 0, maximum precision 38. They must be positive, are limited by the range of the data type, and cannot be null. Adaptive Server Enterprise requires `identity_insert` for explicit inserts and drops, but not for updates to the identity column. The table can contain data when you add an identity column. Adaptive Server Enterprise users cannot explicitly set the next value chosen for an identity column. Adaptive Server Enterprise views cannot contain `IDENTITY/` `AUTOINCREMENT` columns. When using **`SELECT INTO`** under certain conditions, Adaptive Server Enterprise allows Identity/Autoincrement columns in the result table if they were in the table being selected from.

Computed Columns

Computed column support differs as follows:

- SQL Anywhere supports computed columns that can be indexed.
- Adaptive Server Enterprise and SAP Sybase IQ do not.

Temporary Tables

You can create a temporary table by placing a pound sign (#) without an owner specification in front of the table name in a **`CREATE TABLE`** statement. These temporary tables are SAP Sybase IQ-declared temporary tables and are available only in the current connection.

Locating Tables

Physical placement of a table is carried out differently in Adaptive Server Enterprise and SAP Sybase IQ. SAP Sybase IQ supports the **`ON segment-name`** clause, but *segment-name* refers to an SAP Sybase IQ dbspace.

See also

- *Constraints and Defaults with Domains* on page 747

Deleting a Domain

Delete a domain to remove it from the database.

Prerequisites

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP DATATYPE system privilege. • DROP ANY OBJECT system privilege. • You own the domain.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Domains**.
3. Select one or more domains from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple domains.

4. Click **Yes** to confirm deletion.

See also

- *Creating a Domain* on page 746
- *Generating Domain DDL Commands* on page 752
- *Viewing Domain Properties* on page 753
- *Domain Privilege Summary* on page 754
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Domain DDL Commands

Display the data description language SQL code for adding a domain to the database. The SQL code is a useful reference and training tool.

Prerequisites

Database Version	Domain Privileges
SAP Sybase IQ15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, at least one server is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Domains**.
3. Select one or more domains from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple domains.

The DDL view shows the SQL code used to add the selected domains to the database.

See also

- *Creating a Domain* on page 746
- *Deleting a Domain* on page 751
- *Viewing Domain Properties* on page 753
- *Domain Privilege Summary* on page 754
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing Domain Properties

Display the properties for the selected domain.

Prerequisites

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Domains**.
3. Select a domain from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Domain Properties view appears. All property pages are read-only.

See also

- *Creating a Domain* on page 746
- *Deleting a Domain* on page 751
- *Generating Domain DDL Commands* on page 752
- *Domain Privilege Summary* on page 754
- *Authenticating a Login Account for a Managed Resource* on page 282

Domain Privilege Summary

A list of the system privileges and object permissions required to complete the various domain tasks.

Creating a Domain

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • CREATE DATATYPE system privilege. • CREATE ANY OBJECT system privilege.

Deleting a Domain

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP DATATYPE system privilege. • DROP ANY OBJECT system privilege. • You own the domain.

Generating Domain DDL Commands

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing Domain Properties

Database Version	Domain Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

See also

- *Creating a Domain* on page 746
- *Deleting a Domain* on page 751
- *Generating Domain DDL Commands* on page 752
- *Viewing Domain Properties* on page 753

Text Configuration Objects

Create, delete, generate DDL, and manage the properties of text configuration objects.

For detailed information on text configuration objects, in the *SAP Sybase IQ* documentation, see *SAP Sybase IQ Unstructured Data Analytics*.

Creating a Text Configuration Object

Create a text configuration for use with a text index.

Prerequisites

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Text configuration object to be owned by self – Requires RESOURCE authority. Text configuration object to be owned by any user – Requires DBA authority.

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 16.0	<p>Text configuration object to be owned by self – Requires CREATE TEXT CONFIGURATION system privilege.</p> <p>Text configuration object to be owned by any user – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TEXT CONFIGURATION system privilege. • CREATE ANY OBJECT system privilege. <p>Also requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TEXT CONFIGURATION system privilege. • ALTER ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

For detailed information on stoplists, in the *SAP Sybase IQ* documentation, see *SAP Sybase IQ Unstructured Data Analytics > TEXT Indexes and Text Configuration Objects > Text Configuration Objects > Text Configuration Object Settings > Stoplist Setting (STOPLIST)*.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Text Configuration Objects**.
3. Click the arrow next to **Text Configuration Objects** and select **New**.
The Create Text Configuration Wizard appears.
4. On the Text Configuration Name page, specify

Option	Description
Select a resource for which the text configuration will be created	From the list, select the resource for which the text configuration object will be created.
Which user do you want to own the text configuration object?	From the list, select the user to own the text configuration object.
What do you want to name the view?	Enter a unique name for the new text configuration object; maximum of 128 characters.

Option	Description
For which database collation will this text configuration object be used	Each database has a CHAR collation and an NCHAR collation, configured when the database is created. Valid choices are: ISO_BINENG – Binary ordering, English ISO/ASCII 7-bit letter case mappings UCA – Standard default Unicode Collation Algorithm collation Default value is ISO_BINENG.
(Optional) Comment	Specify an option comment for the text configuration object.

5. Click **Next**.
6. On the Choose the Term Breaker page, specify:

Option	Description
Which term breaker algorithm should be used?	Select Generic or N-gram.
What is the minimum term length?	For Generic - Valid range is 1-60. Default value is 1. For N-gram - Not available.
What is the maximum term length?	For Generic - Valid range is 1-60. Default value is 20. For N-gram - Valid range is 1-60. Default value is 4.
Use an external term breaker?	If you chose the database collation ISO_BINENG and Generic term breaker algorithm, you can specify an external library function to break the text into terms, using one of these formats: <ul style="list-style-type: none"> • function-name@library-file-name • Windows-function-name@library-file-name.dll • UNIX:UNIX-function-name@library-file-name.so

7. Click **Next**.
8. (Available for ISO_BINENG database collation only) On the Specify an Option Prefilter page, select **Use an external prefilter** if required and specify the external prefilter function and library.
9. Click **Next**.

10. On the Specify the Stoplist page, indicate the terms to be ignored when building a text index.
11. (Optional) If you chose the Generic term breaker algorithm, you can specify an external library function to break the text into terms. Use one of these formats:
 - function-name@library-file-name
 - Windows-function-name@library-file-name.dll
 - UNIX:UNIX-function-name@library-file-name.so
12. (Optional; available only for CHAR collations) Specify an external library to perform document filtering before term breaker processing.
13. (Optional) Create a stoplist by entering terms to omit from the text index. (Terms in the stoplist are also ignored in queries.) Separate terms with spaces.

Many non-alphanumeric characters are ignored in stoplists; others (including spaces, apostrophes, and dashes) are interpreted as term delimiters. Consequently, including contractions and hyphenated terms may lead to undesirable results, even when you enclose the terms in quotes. How the stoplist is parsed depends on the term breaker and term lengths you specified in step 6.
14. Click **Finish**.

Next

Create a text index that uses your new text configuration.

See also

- *Deleting a Text Configuration Object* on page 758
- *Generating Text Configuration Object DDL Commands* on page 760
- *Viewing or Modifying Text Configuration Object Properties* on page 761
- *Text Configuration Privilege Summary* on page 764
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Text Configuration Object

Remove one or more text configuration objects.

Prerequisites

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Text configuration object owned by self – None required. Table configuration object owned by any user – Requires DBA authority.

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 16.0	<p>Text configuration object owned by self – None required.</p> <p>Table configuration object owned by any user – Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY TEXT CONFIGURATION system privilege. • DROP ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Text Configuration**.
3. Select one or more text configuration objects from the right pane and either.
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Note: You cannot delete the default text configuration objects default_char and or default_nchar.

Tip: Use **Shift-click** or **Control-click** to select multiple text configurations.

4. Click **Yes** to confirm deletion.

See also

- *Creating a Text Configuration Object* on page 755
- *Generating Text Configuration Object DDL Commands* on page 760
- *Viewing or Modifying Text Configuration Object Properties* on page 761
- *Text Configuration Privilege Summary* on page 764
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Text Configuration Object DDL Commands

Generate data description language for one or more text configuration objects. The DDL code can be a useful reference and training tool.

Prerequisites

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Text Configuration**.
3. Select one or more text configuration objects from the right pane and either.
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple text configurations.

The DDL view shows the SQL code used to add the selected text configurations to the database.

See also

- *Creating a Text Configuration Object* on page 755
- *Deleting a Text Configuration Object* on page 758
- *Viewing or Modifying Text Configuration Object Properties* on page 761
- *Text Configuration Privilege Summary* on page 764
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Text Configuration Object Properties

Display and change the properties of a text configuration object for a text index.

Prerequisites

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any text object configuration property page – None required.</p> <p>Modify any text object configuration property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the text configuration object.
SAP Sybase IQ 16.0	<p>View any text object configuration property page – None required.</p> <p>Modify a text configuration object term breaker or external prefilter property – Requires:</p> <ul style="list-style-type: none"> • CREATE ANY EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY TEXT CONFIGURATION system privilege. • ALTER ANY OBJECT system privilege. • You own the text configuration object. <p>Modify a text configuration object comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TEXT CONFIGURATION system privilege. • ALTER ANY TEXT CONFIGURATION system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the text configuration. <p>Modify any other text configuration object properties – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TEXT CONFIGURATION system privilege. • ALTER ANY OBJECT system privilege. • You own the text configuration object.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Text Configuration**.
3. Select a text configuration from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Text Configuration Properties view appears.

4. View or modify the properties.

Note:

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) The name of the text configuration.</p> <p>Type – (Read-only) The type of object.</p> <p>Owner – (Read-only) The owner of the text configuration object.</p> <p>Collation sequence – (Read-only) Type of database collation. Default value is ISO_BINENG. Valid entries are:</p> <ul style="list-style-type: none"> • ISO_BINENG – Binary ordering, English ISO/ASCII 7-bit letter case mappings • UCA – Standard default Unicode Collation Algorithm collation <p>Comment – A text field for adding an optional comment about the text configuration.</p>

Area	Description
Settings	<p>Which term breaker algorithm should be used? – Select Generic or N-gram.</p> <p>What is the minimum term length? – Valid entries are:</p> <ul style="list-style-type: none"> For Generic - Valid range is 1-60. Default value is 1. For N-gram - Not available. <p>What is the maximum term length? – Valid entries are:</p> <ul style="list-style-type: none"> For Generic - Valid range is 1-60. Default value is 20. For N-gram - Valid range is 1-60. Default value is 4. <p>Use an external term breaker? — Available only if Collation sequence is ISO_BINENG and Generic term breaker algorithm are selected.</p> <p>Specify the external term breaker function and library — Specify an external library function to break the text into terms, using one of these formats:</p> <ul style="list-style-type: none"> function-name@library-file-name Windows-function-name@library-file-name.dll UNIX:UNIX-function-name@library-file-name.so <p>Use an external prefilter — Available for ISO_BINENG collation sequence only.</p> <p>Specify the external prefilter function and library — Available for ISO_BINENG collation sequence only.</p>
Stoplist	<p>Indicate the terms to be ignored when building a text index.</p> <p>Sort Terms — Click to sort the term list.</p>
Options (Read-only)	<p>The option settings the text configuration object was created with.</p>

5. Click **OK**.

See also

- *Creating a Text Configuration Object* on page 755
- *Deleting a Text Configuration Object* on page 758
- *Generating Text Configuration Object DDL Commands* on page 760
- *Text Configuration Privilege Summary* on page 764
- *Authenticating a Login Account for a Managed Resource* on page 282

Text Configuration Privilege Summary

A list of the system privileges and object permissions required to complete the various text configuration tasks.

Creating a Text Configuration Object

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Text configuration object to be owned by self – Requires RESOURCE authority. Text configuration object to be owned by any user – Requires DBA authority.
SAP Sybase IQ 16.0	Text configuration object to be owned by self – Requires CREATE TEXT CONFIGURATION system privilege. Text configuration object to be owned by any user – Requires one of: <ul style="list-style-type: none"> • CREATE ANY TEXT CONFIGURATION system privilege. • CREATE ANY OBJECT system privilege. Also requires one of: <ul style="list-style-type: none"> • ALTER ANY TEXT CONFIGURATION system privilege. • ALTER ANY OBJECT system privilege.

Deleting a Text Configuration Object

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Text configuration object owned by self – None required. Table configuration object owned by any user – Requires DBA authority.
SAP Sybase IQ 16.0	Text configuration object owned by self – None required. Table configuration object owned by any user – Requires one of: <ul style="list-style-type: none"> • DROP ANY TEXT CONFIGURATION system privilege. • DROP ANY OBJECT system privilege.

Generating Text Configuration Object DDL Commands

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Text Configuration Object Properties

Database Version	Text Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any text object configuration property page – None required.</p> <p>Modify any text object configuration property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the text configuration object.
SAP Sybase IQ 16.0	<p>View any text object configuration property page – None required.</p> <p>Modify a text configuration object term breaker or external prefilter property – Requires:</p> <ul style="list-style-type: none"> • CREATE ANY EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY TEXT CONFIGURATION system privilege. • ALTER ANY OBJECT system privilege. • You own the text configuration object. <p>Modify a text configuration object comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY TEXT CONFIGURATION system privilege. • ALTER ANY TEXT CONFIGURATION system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the text configuration. <p>Modify any other text configuration object properties – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY TEXT CONFIGURATION system privilege. • ALTER ANY OBJECT system privilege. • You own the text configuration object.

See also

- *Creating a Text Configuration Object* on page 755
- *Deleting a Text Configuration Object* on page 758
- *Generating Text Configuration Object DDL Commands* on page 760
- *Viewing or Modifying Text Configuration Object Properties* on page 761

Text Indexes

Create, delete, generate DDL, and manage the properties of text indexes and text configuration objects. A text index stores positional information for terms in an indexed column. Text indexes are created using settings stored in a text configuration object.

Text indexes significantly speed up full-text searching. You must configure a text index for a table before it is subjected to a full-text search.

Each text index requires a text configuration object. Sybase provides two default text configuration objects, one for CHAR collation, one for NCHAR collation. When you set up a text index, you can use one of the default text configuration objects or create a custom text configuration object.

In the *SAP Sybase IQ* documentation, see *SAP Sybase IQ Unstructured Data Analytics* for detailed information on text indexes.

Creating a Text Index

Set up a text index for a table.

Prerequisites

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• REFERENCE permission on the underlying table being indexed along with CREATE permission on the dbspace where the index is being created.• You own the underlying table being indexed along with CREATE permission on the dbspace where the index is being created. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>

Database Version	Text Index Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege along with CREATE permission on the dbspace where the index is being created. • CREATE ANY OBJECT system privilege. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

- The SAP Sybase IQ resource is authenticated and running.
- The text configuration to be used with a text index already exists.
- You are licensed for the Unstructured Data Analytics option (IQ_UDA).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Text Indexes**.
3. Click the arrow next to **Text Indexes** and select **New**.
The Create Text Index Wizard appears.
4. On the Text Index Name page, specify

Option	Description
Select a resource for which the view will be created	From the list, select the resource for which the text index will be created.

Option	Description
For which table do you want to create the text index?	From the list, select the table.
What do you want to name the text index?	Enter a unique name for the new text index; maximum of 128 characters.

5. Click **Next**.
6. On the Columns page, select the columns to be included in the index.
7. Click **Next**.
8. On the Text Configuration page, select the text configuration object to be included in the index.
If the index is on a main store table, skip to step 11. If the index is on a table in the system store (catalog store), you see a page that lets you select a refresh type.
9. (System store tables only) On the Refresh Type page, specify:

Option	Description
Immediate	The text index is automatically refreshed when data in the underlying table changes.
Manual	The text index is refreshed only when explicitly requested.
Automatic	The text index is automatically refreshed using a time interval that you specify. If you select Automatic, set the interval at which the text index refreshes

Note: If the index is on a main store table, it refreshes automatically whenever the data in the underlying table changes.

10. Click **Next**.
11. On the Dbspace page, select the dbspace in which you want to store the text index.
12. Click **Next**.
13. (Optional) On the Comment page, enter a comment for the text index.
14. Click **Finish** to create the text index.

See also

- *Deleting a Text Index* on page 769
- *Refreshing a Text Index* on page 770
- *Truncating a Text Index* on page 773
- *Generating Text Index DDL Commands* on page 775
- *Viewing or Modifying Text Index Properties* on page 777
- *Text Index Privilege Summary* on page 781

- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Text Index

Remove one or more text indexes.

Prerequisites

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY INDEX system privilege. • DROP ANY OBJECT system privilege. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

- The SAP Sybase IQ resource is authenticated and running.

- You are licensed for the Unstructured Data Analytics option (IQ_UDA).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Text Index**.
3. Select one or more text indexes from the right pane and either.
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple text indexes.

4. Verify that the list of text indexes to be deleted is correct and click **Yes**.

See also

- *Creating a Text Index* on page 766
- *Refreshing a Text Index* on page 770
- *Truncating a Text Index* on page 773
- *Generating Text Index DDL Commands* on page 775
- *Viewing or Modifying Text Index Properties* on page 777
- *Text Index Privilege Summary* on page 781
- *Authenticating a Login Account for a Managed Resource* on page 282

Refreshing a Text Index

Refresh a text index for a system store (IQ catalog store) table to bring it up to date when the underlying data has changed.

Prerequisites

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• REFERENCE permission on the underlying table being indexed.• You own the underlying table being indexed. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>

Database Version	Text Index Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Unstructured Data Analytics option (IQ_UDA).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Text Index**.
3. Select a text index from the right pane and either:
 - Click the arrow to the right of the name and select **Refresh Data**, or
 - From the Administration Console menu bar, select **Resource > Refresh Data**.

Note: If the text is not available for refreshing, the **Refresh Data** button is grayed out.

Tip: Use **Shift-click** or **Control-click** to select multiple text indexes.

4. In the Text Index Refresh Data view, select the isolation level for the refresh:

Level	Description
Read uncommitted (level 0)	<ul style="list-style-type: none"> • Can read rows with or without write lock • Applies no read locks • Data may change during the refresh • Allows dirty reads, nonrepeatable reads, and phantom rows
Read committed (level 1)	<ul style="list-style-type: none"> • Can read only rows with no write lock • Read-locks only the current row and releases it immediately after reading • Data may change during the refresh • Prevents dirty reads • Allows nonrepeatable reads and phantom rows
Repeatable read (level 2)	<ul style="list-style-type: none"> • Can read only rows with no write lock • Read-locks each row as it is read; holds the lock until the refresh is done • Prevents dirty reads and nonrepeatable reads • Allows phantom rows
Serializable (level 3)	<ul style="list-style-type: none"> • Can read only rows with no write lock • Read-locks every row for the duration of the refresh operation • Prevents dirty reads, nonrepeatable reads, and phantom rows
Snapshot	<ul style="list-style-type: none"> • Applies no read locks • Can read any row • The database takes a snapshot of committed data when the refresh operation reads the first row
Share mode (the default)	<ul style="list-style-type: none"> • Allows other transactions to read the underlying table during the refresh operation • Uses shared table locks
Exclusive mode	<ul style="list-style-type: none"> • Does not change the isolation level • Locks the underlying table to ensure that the text index is updated to be consistent with committed data in the table • If an exclusive table lock cannot be obtained, the refresh fails

5. Click **OK** to refresh the text index.

See also

- *Creating a Text Index* on page 766
- *Deleting a Text Index* on page 769

- *Truncating a Text Index* on page 773
- *Generating Text Index DDL Commands* on page 775
- *Viewing or Modifying Text Index Properties* on page 777
- *Text Index Privilege Summary* on page 781
- *Authenticating a Login Account for a Managed Resource* on page 282

Truncating a Text Index

Truncate a text index for a system store (IQ catalog store) table.

Prerequisites

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• ALTER permission on the table being indexed.• You own the underlying table being indexed. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>

Database Version	Text Index Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table being indexed. • You own the underlying table being indexed. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Unstructured Data Analytics option (IQ_UDA).

Task

Truncating lets you delete data from a text index without dropping the text index definition. For example, to modify the stoplist for a text index:

- Truncate the text index.
- Edit the stoplist in the text configuration object associated with the text index.
- Refresh the text index to bring in the new stoplist.

If a text index is set to immediate refresh, you cannot truncate it. Instead, drop it and create a new one.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Schema Objects > Text Index**.
3. Select one or more text indexes from the right pane and either.
 - Click the arrow to the right of the name and select **Truncate Data**, or
 - From the Administration Console menu bar, select **Resource > Truncate Data**.

Note: If the text index is not available for truncating, the **Truncate Data** option is grayed out.

Tip: Use **Shift-click** or **Control-click** to select multiple text indexes.

4. At the confirmation prompt, click **Yes**.

See also

- *Creating a Text Index* on page 766
- *Deleting a Text Index* on page 769
- *Refreshing a Text Index* on page 770
- *Generating Text Index DDL Commands* on page 775
- *Viewing or Modifying Text Index Properties* on page 777
- *Text Index Privilege Summary* on page 781
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Text Index DDL Commands

Generate data description language for one or more text indexes. The DDL code can be a useful reference and training tool.

Prerequisites

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	None required to generate DDL commands; however, requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.

Database Version	Text Index Privileges
SAP Sybase IQ 16.0	<p>None required to generate DDL commands; however,</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Unstructured Data Analytics option (IQ_UDA).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Text Index**.
3. Select one or more text indexes from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

The DDL view shows the SQL code used to add the selected text indexes to the database.

See also

- *Creating a Text Index* on page 766
- *Deleting a Text Index* on page 769
- *Refreshing a Text Index* on page 770
- *Truncating a Text Index* on page 773
- *Viewing or Modifying Text Index Properties* on page 777
- *Text Index Privilege Summary* on page 781

- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Text Index Properties

Display or change the properties of a text index for a main store or catalog store table.

Prerequisites

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p> <p>View text index properties – None required.</p> <p>Rename a text index – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table. • You own the underlying table being indexed. <p>Move a text index – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority. • You own the underlying table being indexed and have CREATE permission on the target dbspace. <p>Modify comment on a text index – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the underlying table being indexed.

Database Version	Text Index Privileges
SAP Sybase IQ 16.0	<p>Requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p> <p>View any text index property page – None required.</p> <p>Rename a text index – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • REFERENCE permission on the underlying table. • You own the underlying table being indexed. <p>Move a text index – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE • One of the following: <ul style="list-style-type: none"> • You own the underlying table being indexed. • REFERENCE permission on the table along with one of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the target dbspace. <p>Modify a text index comment – Requires:</p> <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege. • Also requires one of:

Database Version	Text Index Privileges
	<ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • CREATE ANY OBJECT system privilege. • CREATE ANY INDEX system privilege. • COMMENT ANY OBJECT system privilege. • You own the underlying table being indexed.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Unstructured Data Analytics option (IQ_UDA).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Text Index**.
3. Select a text index from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Text Index Properties view appears.
4. View or modify the properties.

Note:

- When modifying properties, it is not necessary to click **Apply** before changing screens.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.
-

Area	Description
General	<p>Name – The name of the text index.</p> <p>Type – (Read-only) The index type.</p> <p>Table – (Read-only) The table the index uses.</p> <p>Dbospace – (Read-only) The dbospace the text index was created on.</p> <p>Text Configuration Object – (Read-only) The text configuration object used to create the text index.</p> <p>Refresh type – (Read-only) Valid settings are Manual and Automatic. For Automatic, specify the frequency.</p> <p>Last refresh time – (Read-only) The date and time the text index was last refreshed.</p> <p>Refresh Now – If the data has not changed since the last refresh, the refresh date does not change. To force a refresh, truncate the text index, then refresh it. If the text index cannot be manually refreshed, the Refresh Now button is grayed out.</p> <p>Truncate Now – To delete data from a text index without dropping the text index definition. If the text index cannot be truncated, the Truncate Now button is grayed out.</p> <p>Comment – A text field for adding an optional comment about the text index.</p>
Columns (Read-only)	Select a column and click the Details button to view the details of the column.

5. Click **OK**.

See also

- *Creating a Text Index* on page 766
- *Deleting a Text Index* on page 769
- *Refreshing a Text Index* on page 770
- *Truncating a Text Index* on page 773
- *Generating Text Index DDL Commands* on page 775
- *Text Index Privilege Summary* on page 781
- *Authenticating a Login Account for a Managed Resource* on page 282

Text Index Privilege Summary

A list of the system privileges and object permissions required to complete the various text index tasks.

Creating a Text Index

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table being indexed along with CREATE permission on the dbspace where the index is being created. • You own the underlying table being indexed along with CREATE permission on the dbspace where the index is being created. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY INDEX system privilege along with CREATE permission on the dbspace where the index is being created. • CREATE ANY OBJECT system privilege. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

Deleting a Text Index

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY INDEX system privilege. • DROP ANY OBJECT system privilege. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

Refreshing a Text Index

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • REFERENCE permission on the underlying table being indexed. • You own the underlying table being indexed. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

Truncating a Text Index

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • ALTER permission on the table being indexed. • You own the underlying table being indexed. <p>Also requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p>
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • ALTER permission on the table being indexed. • You own the underlying table being indexed. <p>Also requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

Generating Text Index DDL Commands

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	None required to generate DDL commands; however, requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.

Database Version	Text Index Privileges
SAP Sybase IQ 16.0	<p>None required to generate DDL commands; however,</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p>

Viewing or Modifying Text Index Properties

Database Version	Text Index Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes.</p> <p>View text index properties – None required.</p> <p>Rename a text index – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • REFERENCE permission on the underlying table. • You own the underlying table being indexed. <p>Move a text index – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority. • You own the underlying table being indexed and have CREATE permission on the target dbspace. <p>Modify comment on a text index – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the underlying table being indexed.

Database Version	Text Index Privileges
SAP Sybase IQ 16.0	<p>Requires:</p> <ul style="list-style-type: none"> • If the system procedure security model* of the selected database is set to Definer, you require EXECUTE permission on the sa_text_index_stats system procedure to display a list of existing text indexes. • If the system procedure security model* of the selected database is set to Invoker, you require one of the following system privileges to display a list of existing text indexes. <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege • CREATE ANY INDEX system privilege • ALTER ANY INDEX system privilege • DROP ANY INDEX system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • DROP ANY OBJECT system privilege <p>*The system procedure security model of the selected database appears on the General page of database properties.</p> <p>View any text index property page – None required.</p> <p>Rename a text index – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • REFERENCE permission on the underlying table. • You own the underlying table being indexed. <p>Move a text index – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY DBSPACE • One of the following: <ul style="list-style-type: none"> • You own the underlying table being indexed. • REFERENCE permission on the table along with one of the following: <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • CREATE permission on the target dbspace. <p>Modify a text index comment – Requires:</p> <ul style="list-style-type: none"> • MANAGE ANY STATISTICS system privilege. • Also requires one of:

Database Version	Text Index Privileges
	<ul style="list-style-type: none"> • ALTER ANY INDEX system privilege. • ALTER ANY OBJECT system privilege. • CREATE ANY OBJECT system privilege. • CREATE ANY INDEX system privilege. • COMMENT ANY OBJECT system privilege. • You own the underlying table being indexed.

See also

- *Creating a Text Index* on page 766
- *Deleting a Text Index* on page 769
- *Refreshing a Text Index* on page 770
- *Truncating a Text Index* on page 773
- *Generating Text Index DDL Commands* on page 775
- *Viewing or Modifying Text Index Properties* on page 777

Sequence Generators

Sequence generators are used to generate values that are unique across multiple tables, and to generate default values that are something other than the set of natural numbers (1, 2, 3...).

Creating a Sequence Generator

Create a sequence generator on a specified resource.

Prerequisites

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • CREATE ANY SEQUENCE system privilege. • CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Sequence Generators**.
3. Click the arrow next to **Sequence Generators** and select **New**.
The Create Sequence Wizard appears.
4. On the Welcome page of the wizard, specify:

Option	Description
Select a resource for which the sequence generator will be created	Select a resource from the list.
What do you want to name the new sequence generator?	Enter a unique name for the new sequence generator; maximum of 128 characters.
Which user do you want to own the sequence generator?	From the list, select the user designated as the owner of the sequence generator.

5. Click **Next**.
6. On the Values page, specify:

Option	Description
What is the minimum value for this sequence generator?	Enter the minimum value for the sequence generator. Default value is 1. Valid range is -9223372036854775808 to 9223372036854775807.
What is the maximum value for this sequence generator?	Enter the maximum value for the sequence generator. Default value is 9223372036854775807. Valid range is -9223372036854775808 to 9223372036854775807.

7. Click **Next**.
8. On the Increment page, specify:

Option	Description
What is the start value for this sequence generator?	Enter the start value for the sequence generator. Default value is 1. Valid range is -9223372036854775808 to 9223372036854775807.
What is the increment value for this sequence generator?	Enter the incremental value for the sequence generator. Default value is 1. Valid range is -9223372036854775808 to 9223372036854775807.

9. Click **Next**.

10. On the Options page, specify:

Option	Description
Cycle values	(Optional) Select if the sequence generator is to continue generating values [starting over at the start value] once minimum or maximum values have been reached. Option unselected by default.
Cache size	Enter a cache size. The cache size determines the number of preallocated sequence values that are kept in memory for faster access. When the cache is exhausted, it is repopulated and a corresponding entry is written to the transaction log. Default value is 100. Valid range is 0 to unlimited.

11. Click **Next**.

12. (Optional) On the Comment page, specify a comment for the sequence generator.

13. Click **Finish** to create the sequence generator as defined.

See also

- *Deleting a Sequence Generator* on page 790
- *Restarting a Sequence at Start Value* on page 792
- *Generating Sequence Generator DDL Command* on page 793
- *Viewing or Modifying Sequence Generator Properties* on page 794
- *Granting Sequence Generator USAGE Permission* on page 797
- *Revoking Sequence Generator USAGE Permission* on page 798
- *Sequence Generator Privilege Summary* on page 799
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Sequence Generator

Delete one or more sequence generators.

Prerequisites

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the sequence generator.

Database Version	Sequence Generator Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY SEQUENCE system privilege. • DROP ANY OBJECT system privilege. • You own the sequence generator.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Sequence Generators**.
3. Select one or more sequence generators from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple sequence generators.

4. Verify that the list of sequence generators to be deleted is correct and click **Yes**.

See also

- *Creating a Sequence Generator* on page 788
- *Restarting a Sequence at Start Value* on page 792
- *Generating Sequence Generator DDL Command* on page 793
- *Viewing or Modifying Sequence Generator Properties* on page 794
- *Granting Sequence Generator USAGE Permission* on page 797
- *Revoking Sequence Generator USAGE Permission* on page 798
- *Sequence Generator Privilege Summary* on page 799
- *Authenticating a Login Account for a Managed Resource* on page 282

Restarting a Sequence at Start Value

Restart the sequence generator at the start value defined.

Prerequisites

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY SEQUENCE system privilege. • ALTER ANY OBJECT system privilege. • You own the sequence generator.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Sequence Generators**.
3. Select a sequence generator from the right pane and either:
 - Click the arrow to the right of the name and select **Restart At Start Value**, or
 - From the Administration Console menu bar, select **Resource > Restart At Start Value**.
4. At the confirmation prompt, click **Yes**.

See also

- *Creating a Sequence Generator* on page 788
- *Deleting a Sequence Generator* on page 790
- *Generating Sequence Generator DDL Command* on page 793
- *Viewing or Modifying Sequence Generator Properties* on page 794
- *Granting Sequence Generator USAGE Permission* on page 797
- *Revoking Sequence Generator USAGE Permission* on page 798
- *Sequence Generator Privilege Summary* on page 799
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Sequence Generator DDL Command

Generate data description language for one or more sequence generators. The DDL code can be a useful reference and training tool.

Prerequisites

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Sequence Generators**.
3. Select one or more sequence generators from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple sequence generators.

4. The DDL view opens, showing the SQL code used to create the selected sequence generators.

See also

- *Creating a Sequence Generator* on page 788
- *Deleting a Sequence Generator* on page 790
- *Restarting a Sequence at Start Value* on page 792
- *Viewing or Modifying Sequence Generator Properties* on page 794
- *Granting Sequence Generator USAGE Permission* on page 797
- *Revoking Sequence Generator USAGE Permission* on page 798
- *Sequence Generator Privilege Summary* on page 799
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Sequence Generator Properties

View or change the properties of a sequence generator.

Prerequisites

Database Version	Sequence Generator Permissions
SAP Sybase IQ 15.3 and 15.4	<p>View sequence generator properties – None required.</p> <p>Modify a sequence comment – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority. • You own the sequence generator. <p>Modify sequence permissions – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the sequence generator. <p>Modify any other sequence property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the sequence generator.
SAP Sybase IQ 16.0	<p>View any sequence property page – None required.</p> <p>Modify a sequence comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY SEQUENCE system privilege. • ALTER ANY SEQUENCE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. <p>Modify sequence permissions – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the sequence generator. <p>Modify any other sequence property – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY SEQUENCE system privilege. • ALTER ANY OBJECT system privilege. • You own the sequence generator.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Sequence Generators**.
3. Select a sequence generator from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
4. View or modify the properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General page	<p>Name – (Read-only) Name of the selected sequence generator.</p> <p>Owner – (Read-only) Assigned owner of the selected sequence generator.</p> <p>Minimum value – Minimum value for the sequence generator. Default value is 1. Valid range is -9223372036854775808 to 9223372036854775807.</p> <p>Maximum value – Maximum value for the sequence generator. Default value is 1. Valid range is -9223372036854775808 to 9223372036854775807.</p> <p>Start value – Starting value for the sequence generator. Default value is 1. Valid range is -9223372036854775808 to 9223372036854775807.</p> <p>Increment value – Incremental value for the sequence generator. Default value is 1. Valid range is -9223372036854775808 to 9223372036854775807.</p> <p>Cycle values – Select if the sequence generator is to continue generating values [starting over at the start value] once minimum or maximum values have been reached. Option unselected by default.</p> <p>Cache size – Determines the number of preallocated sequence values that are kept in memory for faster access. Default value is 100. Valid range is 0 to unlimited</p> <p>Comment – A text field for adding an optional comment about the sequence generator.</p>
Permissions	See <i>Granting Sequence Generator USAGE Permission</i> on page 797 and <i>Revoking Sequence Generator USAGE Permission</i> on page 798.

5. Click **OK**.

See also

- *Creating a Sequence Generator* on page 788
- *Deleting a Sequence Generator* on page 790
- *Restarting a Sequence at Start Value* on page 792
- *Generating Sequence Generator DDL Command* on page 793
- *Granting Sequence Generator USAGE Permission* on page 797
- *Revoking Sequence Generator USAGE Permission* on page 798
- *Sequence Generator Privilege Summary* on page 799

- *Authenticating a Login Account for a Managed Resource* on page 282

Granting Sequence Generator USAGE Permission

Grant sequence generator usage permission to users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the sequence generator.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Sequence Generators**.
3. Select a sequence generator from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Sequence Generator Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
6. On the Welcome page, indicate whether the permission is being granted to a user or role.
7. Click **Next**.
8. On the Grantees page, select one or more users or roles. Click the box in the header row to select all available users or roles.
9. Click **Next**.

10. On the Permissions page, ensure **Usage** is selected.

11. Click **Finish**.

12. Click **OK**.

See also

- *Creating a Sequence Generator* on page 788
- *Deleting a Sequence Generator* on page 790
- *Restarting a Sequence at Start Value* on page 792
- *Generating Sequence Generator DDL Command* on page 793
- *Viewing or Modifying Sequence Generator Properties* on page 794
- *Revoking Sequence Generator USAGE Permission* on page 798
- *Sequence Generator Privilege Summary* on page 799
- *Authenticating a Login Account for a Managed Resource* on page 282

Revoking Sequence Generator USAGE Permission

Remove sequence generator usage permission from users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the sequence generator.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• <code>MANAGE ANY OBJECT PRIVILEGE</code> system privilege.• You own the sequence generator.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Schema Objects > Sequence Generators**.
3. Select a sequence generator from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The Sequence Generator Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, select a grantee, and click **Revoke**.
6. Click **OK**.

See also

- *Creating a Sequence Generator* on page 788
- *Deleting a Sequence Generator* on page 790
- *Restarting a Sequence at Start Value* on page 792
- *Generating Sequence Generator DDL Command* on page 793
- *Viewing or Modifying Sequence Generator Properties* on page 794
- *Granting Sequence Generator USAGE Permission* on page 797
- *Sequence Generator Privilege Summary* on page 799
- *Authenticating a Login Account for a Managed Resource* on page 282

Sequence Generator Privilege Summary

A list of the system privileges and object permissions required to complete the various sequence generator tasks.

Creating a Sequence Generator

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • CREATE ANY SEQUENCE system privilege. • CREATE ANY OBJECT system privilege.

Deleting a Sequence Generator

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY SEQUENCE system privilege. • DROP ANY OBJECT system privilege. • You own the sequence generator.

Restarting a Sequence at Start Value

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • ALTER ANY SEQUENCE system privilege. • ALTER ANY OBJECT system privilege. • You own the sequence generator.

Generating Sequence Generator DDL Commands

Database Version	Sequence Generator Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Sequence Generator Properties

Database Version	Sequence Generator Permissions
SAP Sybase IQ 15.3 and 15.4	<p>View sequence generator properties – None required.</p> <p>Modify a sequence comment – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE authority. • You own the sequence generator. <p>Modify sequence permissions – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the sequence generator. <p>Modify any other sequence property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the sequence generator.
SAP Sybase IQ 16.0	<p>View any sequence property page – None required.</p> <p>Modify a sequence comment – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY SEQUENCE system privilege. • ALTER ANY SEQUENCE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. <p>Modify sequence permissions – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the sequence generator. <p>Modify any other sequence property – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY SEQUENCE system privilege. • ALTER ANY OBJECT system privilege. • You own the sequence generator.

Granting and Revoking Sequence Generator USAGE Permission

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the sequence generator.

See also

- *Creating a Sequence Generator* on page 788
- *Deleting a Sequence Generator* on page 790
- *Restarting a Sequence at Start Value* on page 792
- *Generating Sequence Generator DDL Command* on page 793
- *Viewing or Modifying Sequence Generator Properties* on page 794
- *Granting Sequence Generator USAGE Permission* on page 797
- *Revoking Sequence Generator USAGE Permission* on page 798

Spatial Support

A spatial reference system describes where local, regional or global features are located. It defines a specific map projection, as well as transformations between different spatial reference systems.

Spatial reference systems only support IQ system store (catalog store) tables. For more information on Spatial Support, in the SAP Sybase IQ documentation, see *SAP Sybase IQ Administration: Spatial Data*.

Creating a Spatial Reference System

Create a spatial reference system on a specified resource.

Prerequisites

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Spatial Support > Spatial Reference Systems**.
3. Click the arrow next to **Spatial Reference Systems** and select **New**. The Create Spatial Reference System Wizard appears.
4. On the Welcome page of the wizard, specify:

Option	Description
Select a resource on which the spatial reference system will be created	Select a resource from the list.
(Multiplex only) Select a multiplex server on which the spatial reference system will be created?	Select a multiplex server from the list.
How would you like to choose the spatial reference system?	Indicate the method to locate predefined the spatial reference system.

5. Click **Next**.

6. Select either a predefined spatial referenced system, or well-known text.

If you select a predefined spatial reference system	<ul style="list-style-type: none"> Browse the list and select a system.
If you select well-known text	<ul style="list-style-type: none"> Paste the well-known text definition and click Validate. The Matching Predefined SRS page appears. Browse the list and select a system.

7. Click **Next**.

8. On the Line Interpretation page:

Option	Description
Line interpretation method	Valid values are: <ul style="list-style-type: none"> Round earth – Geographical or projected spacial reference systems. Planar – Projected spacial reference systems.
Name	Specify a unique name for the spatial reference system to a maximum of 128 characters.
Spatial reference system ID	Specify a unique ID for the spatial reference system. To reduce the possibility of choosing a spatial reference system ID reserved by a defining authority such as OGC or other vendors, do not choose numbers in ranges: <ul style="list-style-type: none"> 0-32,767 (reserved by EPSG) 2,147,483,547-2,147,483,647 (reserved by SAP)

9. Click **Next**.

10. (Optional) On the Comment page, specify a comment for the spatial reference system.

11. Click **Finish**.

See also

- Deleting a Spatial Reference System* on page 805
- Generating Spatial Reference System DDL Commands* on page 806
- Viewing or Modifying Spatial Reference System Properties* on page 807
- Creating a Spatial Unit of Measure* on page 812
- Deleting a Spatial Unit of Measure* on page 815
- Generating Spatial Unit of Measure DDL Commands* on page 816
- Viewing or Modifying Spatial Unit of Measure Properties* on page 817
- Spatial Support Privilege Summary* on page 819
- Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Spatial Reference System

Delete one or more spatial reference systems.

Prerequisites

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • DROP ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Spatial Support > Spatial Reference Systems**.
3. Select one or more spatial reference systems from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple spatial reference systems.

4. Verify that the list of spatial reference systems to be deleted is correct and click **Yes**.

See also

- *Creating a Spatial Reference System* on page 803
- *Generating Spatial Reference System DDL Commands* on page 806
- *Viewing or Modifying Spatial Reference System Properties* on page 807
- *Creating a Spatial Unit of Measure* on page 812
- *Deleting a Spatial Unit of Measure* on page 815
- *Generating Spatial Unit of Measure DDL Commands* on page 816
- *Viewing or Modifying Spatial Unit of Measure Properties* on page 817
- *Spatial Support Privilege Summary* on page 819

- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Spatial Reference System DDL Commands

Generate data description language for one or more spatial reference systems. The DDL code can be a useful reference and training tool.

Prerequisites

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Spatial Support > Spatial Reference Systems**.
3. Select one or more spatial reference systems from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple spatial reference systems.

4. The DDL view opens, showing the SQL code used to create the selected spatial reference systems.

See also

- *Creating a Spatial Reference System* on page 803
- *Deleting a Spatial Reference System* on page 805
- *Viewing or Modifying Spatial Reference System Properties* on page 807
- *Creating a Spatial Unit of Measure* on page 812
- *Deleting a Spatial Unit of Measure* on page 815
- *Generating Spatial Unit of Measure DDL Commands* on page 816
- *Viewing or Modifying Spatial Unit of Measure Properties* on page 817
- *Spatial Support Privilege Summary* on page 819
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Spatial Reference System Properties

View or change the properties of a spatial reference system.

Prerequisites

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View spatial reference system properties – None required.</p> <p>Modify spatial reference system properties or comments – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	<p>View spatial reference system properties – None required.</p> <p>Modify spatial reference system properties – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • ALTER ANY OBJECT system privilege. <p>Modify spatial reference system comment – Requires one of:</p> <ul style="list-style-type: none"> • COMMENT ANY OBJECT system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY SPATIAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Spatial Support > Spatial Reference Systems**.
3. Select a spatial reference system from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
4. View or modify the properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.

- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General page	<p>Name — Name of the selected spatial reference system.</p> <p>Spatial reference system ID — Numeric identifier for your spatial reference system. When you create a spatial reference system based on an existing spatial reference system, set the SRID value to be 1000000000 plus the Well Known value.</p> <hr/> <p>Note: SRSIDs 0, 2147483646, and 2147483647 are restricted.</p> <hr/> <p>Organization — The name of the organization that defined the spatial reference system.</p> <p>Organization coordinate reference system ID — The integer identifier assigned by the organization that defined the spatial reference system.</p> <p>Comment — A text field for adding an optional comment about the spatial reference system.</p>

Area	Description
Settings page	<p>Spatial reference system type — Either Geographic or Non-geographic.</p> <p>Line interpretation — (Applies only to geographic spatial reference system type.)</p> <ul style="list-style-type: none"> • Round earth — Round-earth spatial reference systems use an ellipsoid to represent the Earth. Points are mapped to the ellipsoid for computations, all lines follow the shortest path and arc toward the pole, and geometries can cross the date line. • Planar — Flat-earth, or planar, reference systems project all or a portion of the surface of the Earth to a flat, two dimensional plane (planar), and use a simple 2D Euclidean geometry. Lines between points are straight (except for circularstrings), and geometries cannot wrap over the edge (cross the dateline). <p>Axis order — Order of axis in the spatial reference system; for example: Long . / Lat . / Z/M. Not editable.</p> <p>Polygon format — Specifies the orientation of polygon rings of the input data. Internally, SAP Sybase IQ interprets polygons by looking at the orientation of the constituent rings. As one travels a ring in the order of the defined points, the inside of the polygon is on the left side of the ring. The same rules are applied in planar and round earth spatial reference systems.</p> <ul style="list-style-type: none"> • Counterclockwise — The input follows SAP Sybase IQ's internal interpretation: the inside of the polygon is on the left side while following ring orientation. • Clockwise — The input follows the opposite of SAP Sybase IQ's approach: the inside of the polygon is on the right side while following ring orientation. • EvenOdd — (Default) The orientation of rings is ignored and the inside of the polygon is instead determined by looking at the nesting of the rings, with the exterior ring being the largest ring and interior rings being smaller rings inside this ring. A ray is traced from a point within the rings and radiating outward crossing all rings. If the number the ring being crossed is an even number, it is an outer ring. If it is odd, it is an inner ring. <p>Storage format — When you insert spatial data into the database from an external format (such as WKT or WKB), the database server normalizes the data to improve the performance and semantics of spatial operations. The normalized representation may differ from the original representation (for example, in the orientation of polygon</p>

Area	Description
	<p>rings or the precision stored in individual coordinates). While spatial equality is maintained after the normalization, some original input characteristics may not be reproducible, such as precision and ring orientation. In some cases you may want to store the original representation, either exclusively, or in addition to the normalized representation.</p> <ul style="list-style-type: none"> • Internal — The database server stores only the normalized representation. Specify this value when the original input characteristics do not need to be reproduced. This is the default for planar spatial reference systems. <p>Original — The database server stores only the original representation. The original input characteristics can be reproduced, but all operations on the stored values must repeat normalization steps, possibly slowing down operations on the data.</p> <p>Mixed — The database server stores the internal version and, if it is different from the original version, it stores the original version as well. By storing both versions, the original representation characteristics can be reproduced and operations on stored values do not need to repeat normalization steps. However, storage requirements may increase significantly because potentially two representations are being stored for each geometry.</p> <p>Semi-major axis — (Applies only to geographic spatial reference system type.) The Earth is not a perfect sphere because the rotation of the Earth causes a flattening so that the distance from the center of the Earth to the North or South pole is less than the distance from the center to the equator. For this reason, the Earth is modeled as an ellipsoid with different values for the semi-major axis (distance from center to equator) and semi-minor axis (distance from center to the pole). It is most common to define an ellipsoid using the semi-major axis and the inverse flattening, but it can instead be specified using the semi-minor axis (for example, this approach must be used when a perfect sphere is used to approximate the Earth).</p> <p>Inverse flattening — (Applies only to geographic spatial reference system type.) The inverse flattening (1/f) is a ratio:</p> $1/f = (\text{semi-major-axis}) / (\text{semi-major-axis} - \text{semi-minor-axis})$ <p>f measures symmetry axis compression relative to the equatorial radius of the ellipsoid.</p>

Area	Description
Coordinates page	<p>Latitude — (Applies only to geographic spatial reference system type.)</p> <ul style="list-style-type: none"> • Bounded between north — North boundary. • and south — South boundary. • Unbounded — Area is not bounded. <p>Longitude — (Applies only to geographic spatial reference system type.)</p> <ul style="list-style-type: none"> • Bounded between west — West boundary. • and east — East boundary. • Unbounded — Area is not bounded. <p>X — (Applies only to non-geographic spatial reference system type.) X-coordinate value of a geometry.</p> <ul style="list-style-type: none"> • Bounded between minimum — Minimum value. • and maximum — Maximum value. • Unbounded — Area is not bounded. <p>Y — (Applies only to non-geographic spatial reference system type.) Y-coordinate value of a geometry.</p> <ul style="list-style-type: none"> • Bounded between minimum — Minimum value. • and maximum — Maximum value. • Unbounded — Area is not bounded. <p>Z — Z-coordinate value of a geometry.</p> <ul style="list-style-type: none"> • Bounded between minimum — Minimum value. • and maximum — Maximum value. • Unbounded — Area is not bounded. <p>M — M-coordinate value of a geometry.</p> <ul style="list-style-type: none"> • Bounded between minimum — Minimum value. • and maximum — Maximum value. • Unbounded — Area is not bounded. <p>Snap to grid — (Planar line interpretation only.) The action of positioning the points in a geometry so they align with intersection points on a grid. When aligning a point with the grid, the X and Y values may be shifted by a small amount - similar to rounding. In the context of spatial data, a grid is a framework of lines that is laid down over a two-dimensional representation of a spatial reference system..</p> <p>Tolerance — Tolerance defines the distance within which two points or parts of geometries are considered equal. This can be thought of as</p>

Area	Description
	<p>all geometries being represented by points and lines drawn by a marker with a thick tip, where the thickness is equal to the tolerance. Any parts that touch when drawn by this thick marker are considered equal within tolerance. If two points are exactly equal to tolerance apart, they are considered not equal within tolerance.</p> <p>Linear unit of measure — Select a unit of measure.</p> <p>Angular unit of measure — Select a unit of measure.</p>
Transform definition	Transform definition — The spatial reference system transform definition text. Not editable.

5. Click **OK**.

See also

- *Creating a Spatial Reference System* on page 803
- *Deleting a Spatial Reference System* on page 805
- *Generating Spatial Reference System DDL Commands* on page 806
- *Creating a Spatial Unit of Measure* on page 812
- *Deleting a Spatial Unit of Measure* on page 815
- *Generating Spatial Unit of Measure DDL Commands* on page 816
- *Viewing or Modifying Spatial Unit of Measure Properties* on page 817
- *Spatial Support Privilege Summary* on page 819
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Spatial Unit of Measure

Create the unit of measure by which the spatial reference system measures coordinates.

Prerequisites

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • MANAGE ANY SPATIAL OBJECT.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Spatial Support > Units of Measure**.
3. Click the arrow next to **Spatial Units of Measure** and select **New**.
The Create Spatial Unit of Measure Wizard appears.
4. On the Welcome page of the wizard, specify:

Option	Description
Select a resource on which the spatial unit of measure will be created	Select a resource from the list.
(Multiplex only) Select a multiplex server on which the unit of measure will be created.	Select a resource from the list.
How would you like to create the unit of measure?	Indicate the method for creating the unit of measure; either choosing from a list of predefined units of measure, or creating a custom unit of measure.

5. Click **Next**.
6. (Predefined units of measure only) On the Unit Selection page of the wizard, filter the columns to locate the desired unit of measure. Highlight the unit of measure.
(Custom units of measure only) On the Custom Setting page of the wizard, specify:

Option	Description
Provide a name for the custom unit of measure	Specify a name for the unit of measure.

Option	Description
Which type of unit of measure do you want to create?	<ul style="list-style-type: none"> • Linear – If you are using a projected coordinate system, the individual coordinate values represent a linear distance along the surface of the Earth to a point. Coordinate values can be measured by the meter, foot, mile, or yard. The projected coordinate system must explicitly state the linear unit of measure in which the coordinate values are expressed. Meter, metre, and planar degree are linear units of measure. • Angular – Geographic features can be measured in degrees of latitude, radians, or other angular units of measure. Every spatial reference system must explicitly state the name of the unit in which geographic coordinates are measured, Radian and degree are angular units of measure.
Specify the custom unit of measure's conversion factor to another unit of measure of the same type.	<ul style="list-style-type: none"> • <text box> XXX – Specify the number of units of your custom unit of measure. • = <text box> – Specify the number of radians (select the radian type in the pull-down) equal to your specified number of custom units of measure. <p>Every spatial reference system must explicitly state the name of the unit in which geographic coordinates are measured, and must include the conversion from the specified unit to a radian.</p>

See also

- *Creating a Spatial Reference System* on page 803
- *Deleting a Spatial Reference System* on page 805
- *Generating Spatial Reference System DDL Commands* on page 806
- *Viewing or Modifying Spatial Reference System Properties* on page 807
- *Deleting a Spatial Unit of Measure* on page 815
- *Generating Spatial Unit of Measure DDL Commands* on page 816
- *Viewing or Modifying Spatial Unit of Measure Properties* on page 817
- *Spatial Support Privilege Summary* on page 819
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Spatial Unit of Measure

Delete one or more spatial units of measure.

Prerequisites

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • DROP ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Spatial Support > Units of Measure**.
3. Select one or more spatial units of measure systems from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple units of measure.

4. Verify that the list of units of measure to be deleted is correct and click **Yes**.

See also

- *Creating a Spatial Reference System* on page 803
- *Deleting a Spatial Reference System* on page 805
- *Generating Spatial Reference System DDL Commands* on page 806
- *Viewing or Modifying Spatial Reference System Properties* on page 807
- *Creating a Spatial Unit of Measure* on page 812
- *Generating Spatial Unit of Measure DDL Commands* on page 816
- *Viewing or Modifying Spatial Unit of Measure Properties* on page 817
- *Spatial Support Privilege Summary* on page 819

- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Spatial Unit of Measure DDL Commands

Generate data description language for one or more spatial units of measure. The DDL code can be a useful reference and training tool.

Prerequisites

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Spatial Support > Unit of Measure**.
3. Select one or more spatial units of measure from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple spatial units of measure.

4. The DDL view opens, showing the SQL code used to create the selected spatial units of measure.

See also

- *Creating a Spatial Reference System* on page 803
- *Deleting a Spatial Reference System* on page 805
- *Generating Spatial Reference System DDL Commands* on page 806
- *Viewing or Modifying Spatial Reference System Properties* on page 807
- *Creating a Spatial Unit of Measure* on page 812
- *Deleting a Spatial Unit of Measure* on page 815
- *Viewing or Modifying Spatial Unit of Measure Properties* on page 817
- *Spatial Support Privilege Summary* on page 819
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Spatial Unit of Measure Properties

View or change the properties of a spatial unit of measure.

Prerequisites

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View spatial unit of measure properties – None required.</p> <p>Modify spatial unit of measure properties or comments – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	<p>View any spatial unit of measure property page – None required.</p> <p>Modify a spatial unit of measure comment – Requires one of:</p> <ul style="list-style-type: none"> • COMMENT ANY OBJECT system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY SPATIAL OBJECT system privilege. <p>Modify any other spatial unit of measure property – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • ALTER ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Schema Objects > Spatial Support > Unit of Measure**.
3. Select a spatial unit of measure from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
4. View or modify properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.

- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General page	<p>Name — Name of the selected spatial unit of measure.</p> <p>Unit type — Either linear or angular. Meter, metre, and planar degree are linear units of measure. Radian and degree are angular units of measure. Not editable for degree, meter, metre, planar degree, or radian.</p> <p>Conversion factor — The unit of measure's conversion factor to another unit of measure of the same type. Must be a double-precision floating-point value. Not editable for degree, meter, metre, planar degree, or radian</p> <p>Comment — A text field for adding an optional comment about the spatial unit of measure.</p>

5. Click **OK**.
6. Click **Next**.
7. (Optional) On the Comment page, specify a comment for the spatial unit of measure.
8. Click **Finish**.

See also

- *Creating a Spatial Reference System* on page 803
- *Deleting a Spatial Reference System* on page 805
- *Generating Spatial Reference System DDL Commands* on page 806
- *Viewing or Modifying Spatial Reference System Properties* on page 807
- *Creating a Spatial Unit of Measure* on page 812
- *Deleting a Spatial Unit of Measure* on page 815
- *Generating Spatial Unit of Measure DDL Commands* on page 816
- *Spatial Support Privilege Summary* on page 819
- *Authenticating a Login Account for a Managed Resource* on page 282

Spatial Support Privilege Summary

A list of the system privileges and object permissions required to complete the various spatial support tasks.

Creating a Spatial Reference System

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • CREATE ANY OBJECT system privilege.

Deleting a Spatial Reference System

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • DROP ANY OBJECT system privilege.

Generating Spatial Reference System DDL Commands

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Spatial Reference System Properties

Database Version	Spatial Reference System Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View spatial reference system properties – None required.</p> <p>Modify spatial reference system properties or comments – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	<p>View spatial reference system properties – None required.</p> <p>Modify spatial reference system properties – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • ALTER ANY OBJECT system privilege. <p>Modify spatial reference system comment – Requires one of:</p> <ul style="list-style-type: none"> • COMMENT ANY OBJECT system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY SPATIAL OBJECT system privilege.

Creating a Spatial Unit of Measure

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY OBJECT system privilege. • MANAGE ANY SPATIAL OBJECT.

Deleting a Spatial Unit of Measure

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • DROP ANY OBJECT system privilege.

Generating Spatial Unit of Measure DDL Commands

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Spatial Unit of Measure Properties

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 15.3 and 15.4	View spatial unit of measure properties – None required. Modify spatial unit of measure properties or comments – Requires one of: <ul style="list-style-type: none"> • DBA authority. • You are a member of the SYS_SPATIAL_ADMIN_ROLE group.

Database Version	Spatial Unit of Measure Privileges
SAP Sybase IQ 16.0	<p>View any spatial unit of measure property page – None required.</p> <p>Modify a spatial unit of measure comment – Requires one of:</p> <ul style="list-style-type: none"> • COMMENT ANY OBJECT system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • MANAGE ANY SPATIAL OBJECT system privilege. <p>Modify any other spatial unit of measure property – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY SPATIAL OBJECT system privilege. • ALTER ANY OBJECT system privilege.

See also

- *Creating a Spatial Reference System* on page 803
- *Deleting a Spatial Reference System* on page 805
- *Generating Spatial Reference System DDL Commands* on page 806
- *Viewing or Modifying Spatial Reference System Properties* on page 807
- *Creating a Spatial Unit of Measure* on page 812
- *Deleting a Spatial Unit of Measure* on page 815
- *Generating Spatial Unit of Measure DDL Commands* on page 816
- *Viewing or Modifying Spatial Unit of Measure Properties* on page 817

Security and User Management

Security encompasses the areas of user, authentication and login management.

Sybase Control Center administration supports SAP Sybase IQ database versions 15.3 or later. Security for versions 15.3 and 15.4 uses authority-based security, while 16.0 uses role-based security.

Authority-Based and **Role-Based** and their sub items appear in the Administration Console regardless of the managed resources selected. However, the functionality of the underlying items is dependant on the version of the managed resource. If the item selected is not supported by the managed resource version, the right pane remains empty. For example, if the managed resource is 16.0 and you select **IQ Server > Security > Authority-Based > Groups**, nothing appears in the right pane.

In the same Administration Console, it is possible to display multiple managed resources, encompassing multiple versions. Under this scenario, only version supported information for the selected item appears in the right pane. For example, managed resource A (version 15.4) and managed resource C (version 16.0) are displayed in the same Administration Console.

When you select **IQ Server > Security > Role-Based > Standalone Roles**, the information that appears only pertains to resource C, since resource A does not support standalone roles.

Users is common to both **Authority-Based** and **Role-Based**. When managing users, remember that it is possible for the same user ID to exist in multiple databases, for the same or different versions. In an Administration Console displaying multiple resources, a user ID can be listed multiple times. Always check the Server column value for the selected user ID before making changes.

In the Administration Console, to display the list of selected managed resources and their corresponding database version number, click **Resource Selection** (below the Administration Console menu bar). To hide the display, click **Navigation** (scroll to the bottom of the view).

Note: Clicking **Resource Selection** does not toggle the display on or off.

Authority-Based Security

Manage users, groups and database authorities.

Authority-based security is supported with database versions 15.3 and 15.4 only.

Authority-Based Users

Add, change, and delete users.

Users are objects within the database.

See also

- *Configuring SAP Sybase IQ Authority-Based Users for Monitoring* on page 128

Creating an Authority-Based User

Add a new user to the database using the Create User wizard.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • Both USER ADMIN and PERMS ADMIN authorities.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.

Task

All new users are automatically added to the PUBLIC group.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Click the arrow next to **Users** and select **New**.
The Create User Wizard appears.
4. On the Welcome page, specify

Option	Description
Select a resource for which the user will be created:	Select a resource from the list. Note: If the selected resource does not support authority-based security, an error message appears.
What do you want to name the new user?	Enter a name for the new user.

5. Click **Next**.
6. On the Specify a Password page:

Option	Description
Enable password	Allows the user to connect to the database with password security. Leave this option unselected to disable the password and confirm password options.
Password	The password for the user. Characters appear as asterisks.
Confirm password	Confirms the password. The contents of the two password fields must match exactly.
Requires password change on next login	Forces the user to change the password at the next login.
Login policy	Select a login policy from the list.

7. Click **Next**.
8. On the Select Authorities page, select one or more the authorities you want to assign to the new user:

Authority	Description
Backup	Allows this user to back up the database.
DBA	Grants DBA authority to administer the database.
Multiplex Admin	Grants Multiplex Admin authority to the user; Multiplex Admin authority allows a user to perform multiplex administration tasks.
Operator	Grants Operator authority to the user; Operator authority lets a user checkpoint databases, drop connections, backup databases, and monitor the system.
Perms Admin	Grants Perms Admin authority to the user; Perms Admin authority lets a user manage data permissions, groups, authorities, and passwords.
Profile	Allows this user to perform application and procedure profiling, and request log creation, and analysis. Profile authority is also required by the index consultant.
Read client file	Allows this user to read from a file on the client computer.
Read file	Grants Read file authority to the user, allowing the user to execute SELECT statements against a file using the OPENSTRING clause.
Remote DBA	Grants Remote DBA authority to any table the user can access. To ensure that actions are secure, run the SQL Remote Message agent using a user ID with this type of authority.
Resource	Grants resource authority to the user; resource authority lets a user create database objects.
Space Admin	Grants Space Admin authority to the user; Space Admin authority lets a user manage dbspaces.
User Admin	Grants User Admin authority to the user; User Admin authority lets a user manage users, external logins, and login policies.
Validate	Allows this user to validate tables, materialized views, and indexes.
Write client file	Allows this user to write to a file on the client computer.

9. Click **Next**.

10. (Optional) On the Specify a comment page, enter a comment for this user.

11. Click **Finish**.

See also

- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827

- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting an Authority-Based User

Delete a user from the database.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• USER ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Select one or more users from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple users.

4. Click **Yes** to confirm deletion.

See also

- *Creating an Authority-Based User* on page 823
- *Converting an Authority-Based User to a Group* on page 827
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Converting an Authority-Based User to a Group

Change an existing user into a group that retains the user's authorities.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Change to Group**, or
 - From the Administration Console menu bar, select **Resource > Change to Group**.

4. Click **Yes** to confirm the change.

The user disappears from the Users list and appears on the Groups list.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Authority-Based User Options

View or change database option settings assigned to a user.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.

Task

For database options that can be set at either level, when set at the user level, the setting overrides the current value for that user only. When set it at the database level, the value becomes the new default, and is applied to any existing users who have not had the option overridden at the user level.

For information on the level at each option can be set and the system privilege required, in the SAP Sybase IQ 15.x documentation, see the alphabetical list of Database options in *SAP Sybase IQ Reference: Statements and Options*.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Options**, or
 - From the Administration Console menu bar, select **Resource > Options**.

A list of the current settings of each option appears.

4. To change a setting, click in the Setting column for the option and enter the new value.
5. Choose one of the following:
 - Click **Apply** to save the change and continue modifying options.
 - Click **OK** to save all changes and close the Options view.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Authority-Based User DDL Commands

Display the SQL data description language for creating a user. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Select one or more users from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple users.

The DDL view opens, showing the SQL code used to create the selected authority-based users.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Authority-Based User Properties

View or change the details of login parameters and authorities for authority-based users.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	<p>View any user property page – None required.</p> <p>Modify a password – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. • PERMS ADMIN authority. <p>Modify a login policy – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. <p>Modify any other user property except those relating to permissions –</p> <ul style="list-style-type: none"> • Requires DBA authority. <p>For privileges relating to user permissions, see:</p> <ul style="list-style-type: none"> • <i>Authority-Based Database Object Permissions Privilege Summary</i> on page 889
SAP Sybase IQ 16.0	Not Supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties view appears

4. View or edit the properties.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) Name of the user.</p> <p>Enable Password – Allows the user to connect to the database with password security. Clearing this option disables the Password and Confirm Password options. User can log on without specifying a password.</p> <p>Password – The password for the user. Characters appear as asterisks.</p> <p>Confirm password – A field for confirming the password that you typed in the Password text box. The contents of the two fields must match exactly.</p> <p>Password creation time – Date and time when the password was created.</p> <p>Change password on next login – Select to force the user to change the password at the next login.</p> <p>Login policy – Select a login policy for the user from the list.</p> <p>Last login time – (Read-only) Last time the user successfully logged in.</p> <p>Failed login attempts – (Read-only) Number of times the user has tried to log in with an incorrect password.</p> <p>Locked – (Read-only) Displays false if the account is unlocked. Displays true if the user has exceeded the allowed number of failed login attempts.</p> <p>Unlock now – Unlocks the account if Locked is true.</p> <p>Comment – A text field for adding an optional comment about the user.</p>

Area	Description
Authorities	<p>Backup - Grants the ability to perform database backups.</p> <p>DBA - Grants the ability fully administer the database.</p> <p>Multiplex Admin - Grants the ability for Multiplex server administration.</p> <p>Operator - Grants the ability to backup and checkpoint databases, perform system monitoring, and drop connections.</p> <p>Perms Admin - Grants the ability to manage data permission, groups, authorities, and passwords.</p> <p>Profile - Grants the ability to perform application and procedure profiling, request log creation and analysis, and by the Index Consultant.</p> <p>Read client file - Grants the ability to read from a file on the client computer, for example when loading data.</p> <p>Read file - Grants the ability to the group to execute SELECT statements against a file using the OPENSTRING clause.</p> <p>Remote DBA - Grants Remote DBA authority to any table the group can access. To ensure that actions are secure, run the SQL Remote Message agent using a user ID with this type of authority.</p> <p>Resource - Grants the ability to create database objects.</p> <p>Space Admin - Grants the ability to perform dbspace management (including CREATE permission) and read-only selective database restoration.</p> <p>User Admin - Grants the ability to manage users, external logins, and login policies management.</p> <p>Validate - Grants the ability to validate tables, materialized views, and indexes.</p> <hr/> <p>Note: Materialized views are only supported for tables in the IQ system store.</p> <hr/> <p>Write client file - Grants the ability to write to a file on the client computer, for example when downloading data.</p>
LDAP	Feature not supported in authority-based security model.
Permission	See <i>Authority-Based User and Group Object Permissions</i> on page 865.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Changing an Authority-Based User Password* on page 834
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing an Authority-Based User Password

Change the password for another authority-base user.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties page appears.

4. On the General Properties page, type the new password in the Password and Confirm password fields.
5. Click **OK**.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Forcing an Authority-Based User to Change their Password

Force an authority-based user to change their password on next log in.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Select a user from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The User Properties page appears.

4. On the General Properties page, select **Require password change on next login**.
5. Click **OK**.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Unlocking an Authority-Based User Account

Unlock a locked authority-based user account.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• USER ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties page appears.

4. On the General Properties page, select **Unlock Now**.
5. Click **OK**.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing an Authority-Based User Login Policy

Assign an authority-based user a different login policy

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority- Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties page appears.

4. Select a new login policy from the list.
5. Click **OK**.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Adding an Authority to an Authority-Based User

Add authorities to a user to allow him or her to perform specified database operations, such as the ability to manage dbspaces.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties view appears

4. In the left pane, click **Authorities**.
5. In the right pane, select one or more authorities:

Authority	Description
Backup	Grants the ability to perform database backups.
DBA	Grants the ability fully administer the database.
Multiplex Admin	Grants the ability for Multiplex server administration
Operator	Grants the ability to backup and checkpoint databases, perform system monitoring, and drop connections.

Authority	Description
Perms Admin	Grants the ability to manage data permission, groups, authorities, and passwords.
Profile	Grants the ability to perform application and procedure profiling, request log creation and analysis, and by the Index Consultant.
Read client file	Grants the ability to read from a file on the client computer, for example when loading data.
Read file	Grants the ability to the group to execute SELECT statements against a file using the OPENSTRING clause.
Remote DBA	Grants Remote DBA authority to any table the group can access. To ensure that actions are secure, run the SQL Remote Message agent using a user ID with this type of authority.
Resource	Grants the ability to create database objects.
Space Admin	Grants the ability to perform dbspace management (including CREATE permission) and read-only selective database restoration.
User Admin	Grants the ability to manage users, external logins, and login policies management.
Validate	Grants the ability to validate tables, materialized views, and indexes.
Write client file	Grants the ability to write to a file on the client computer, for example when downloading data.

6. Click **Apply** to save your changes and continue granting authorities, or click **OK** to save and close the properties view.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Removing an Authority from an Authority-Based User* on page 841

- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing an Authority from an Authority-Based User

Remove a user's ability to perform specific authorized database operations.

Prerequisites

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties view appears

4. In the left pane, click **Authorities**.
5. Clear the check box beside the authorities you want to revoke from the user.
6. Click **Apply** to save your changes and keep revoking authorities, or click **OK** to save and close the properties view.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834

- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Authority-Based User Privilege Summary* on page 842
- *Authenticating a Login Account for a Managed Resource* on page 282

Authority-Based User Privilege Summary

A list of the system privileges and object permissions required to complete the various authority-based user tasks.

Creating an Authority-Based User

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• Both USER ADMIN and PERMS ADMIN authorities.
SAP Sybase IQ 16.0	Not supported.

Deleting an Authority-Based User

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• USER ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Converting an Authority-Based User to a Group

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Viewing or Modifying Authority-Based User Options

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Not supported.

Generating Authority-Based User DDL Commands

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	Not supported.

Viewing or Modifying Authority-Based User Properties

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	<p>View any user property page – None required.</p> <p>Modify a password – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. • PERMS ADMIN authority. <p>Modify a login policy – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. <p>Modify any other user property except those relating to permissions –</p> <ul style="list-style-type: none"> • Requires DBA authority. <p>For privileges relating to user permissions, see:</p> <ul style="list-style-type: none"> • <i>Authority-Based Database Object Permissions Privilege Summary</i> on page 889
SAP Sybase IQ 16.0	Not Supported.

Changing an Authority-Based User Password

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

Forcing an Authority-Based User Password Change

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

Unlocking an Locked Authority-Based User Account

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

Changing an Authority-Based User Login Policy

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not Supported.

Granting or Revoking an Authority from a User

Database Version	Authority-Based User Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

See also

- *Creating an Authority-Based User* on page 823
- *Deleting an Authority-Based User* on page 826
- *Converting an Authority-Based User to a Group* on page 827
- *Viewing or Modifying Authority-Based User Options* on page 828
- *Generating Authority-Based User DDL Commands* on page 829
- *Viewing or Modifying Authority-Based User Properties* on page 831
- *Changing an Authority-Based User Password* on page 834
- *Forcing an Authority-Based User to Change their Password* on page 835
- *Unlocking an Authority-Based User Account* on page 836
- *Changing an Authority-Based User Login Policy* on page 837
- *Adding an Authority to an Authority-Based User* on page 839
- *Removing an Authority from an Authority-Based User* on page 841

Authority-Based Groups

Add, change, and delete authority-based groups containing users and/or other groups.

Both users and groups are objects within the database. Groups are also containers for containing users and other groups. Think of a group as a user ID with special permissions, such as the ability to have members. You grant and revoke authorities for a group in exactly the same manner as you do for users.

For most databases, manage authorities by using groups, rather than by assigning authorities to individual users one at a time.

Creating an Authority-Based Group

Add a new group to the database using the Create Group wizard.

Prerequisites

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • Both USER ADMIN and PERMS ADMIN authorities
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Groups**.
3. Click the arrow next to **Groups** and select **New**.
The Create Group Wizard appears.
4. On the Welcome page, specify:

Option	Description
Select a resource for which the group will be created:	Select a resource from the list. Note: If the selected resource does not support authority-based security, an error message appears.
What do you want to name the new group?	Enter a unique name for the new group.

5. Click **Next**.
6. On the Specify a Password page, specify:

Area	Description
Enable password	Select to allow the group to connect to the database with password security. Leave this option unselected to disable the password and confirm password options.

Area	Description
Password	Enter the password for the group. Characters appear as asterisks when typed.
Confirm password	Confirms the password. The contents of the two password fields must match exactly.
Requires password change on next login	Select to force a password change the next time the group logs in. Characters appear as asterisks when typed.
Login policy	Select a login policy from the list.

7. Click **Next**.
8. On the **Select Authorities** page, select the authorities you want to assign to the new group:

Authority	Description
Backup	Grants the ability to perform database backups.
DBA	Grants the ability fully administer the database.
Multiplex Admin	Grants the ability for Multiplex server administration
Operator	Grants the ability to backup and checkpoint databases, perform system monitoring, and drop connections.
Perms Admin	Grants the ability to manage data permission, groups, authorities, and passwords.
Profile	Grants the ability to perform application and procedure profiling, request log creation and analysis, and by the Index Consultant.
Read client file	Grants the ability to read from a file on the client computer, for example when loading data.
Read file	Grants the ability to the group to execute SELECT statements against a file using the OPENSTRING clause.
Remote DBA	Grants Remote DBA authority to any table the group can access. To ensure that actions are secure, run the SQL Remote Message agent using a user ID with this type of authority.
Resource	Grants the ability to create database objects.
Space Admin	Grants the ability to perform dbspace management (including CREATE permission) and read-only selective database restoration.

Authority	Description
User Admin	Grants the ability to manage users, external logins, and login policies management.
Validate	Grants the ability to validate tables, materialized views, and indexes.
Write client file	Grants the ability to write to a file on the client computer, for example when downloading data.

9. Click **Next**.

10. (Optional) On the Specify a comment page, enter a comment for this user.

11. Click **Finish**.

See also

- *Deleting an Authority-Based Group* on page 848
- *Converting an Authority-Based Group to a User* on page 849
- *Adding Authority-Based Users and Groups to Groups* on page 850
- *Removing Authority-Based Users or Groups from a Group* on page 852
- *Viewing or Modifying Authority-Based Group Options* on page 853
- *Generating Authority-Based Group DDL Commands* on page 854
- *Viewing or Modifying Authority-Based Group Properties* on page 855
- *Adding an Authority to a Group* on page 859
- *Removing an Authority from a Group* on page 861
- *Authority-Based Group Privilege Summary* on page 862
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting an Authority-Based Group

Delete a group from the database.

Prerequisites

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Groups**.
3. Select one or more groups from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple groups.

Note: Some groups cannot be deleted. If at least one of the selected groups cannot be deleted, the **Delete** option becomes unavailable.

4. Click **Yes** to confirm deletion.

See also

- *Creating an Authority-Based Group* on page 846
- *Converting an Authority-Based Group to a User* on page 849
- *Adding Authority-Based Users and Groups to Groups* on page 850
- *Removing Authority-Based Users or Groups from a Group* on page 852
- *Viewing or Modifying Authority-Based Group Options* on page 853
- *Generating Authority-Based Group DDL Commands* on page 854
- *Viewing or Modifying Authority-Based Group Properties* on page 855
- *Adding an Authority to a Group* on page 859
- *Removing an Authority from a Group* on page 861
- *Authority-Based Group Privilege Summary* on page 862
- *Authenticating a Login Account for a Managed Resource* on page 282

Converting an Authority-Based Group to a User

Change an existing group into a user.

Prerequisites

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Groups**.
3. Select a group from the right pane and either:
 - Click the arrow to the right of the name and select **Change to user**, or
 - From the Administration Console menu bar, select **Resource > Change to user**.
4. Click **Yes** to confirm the change.

See also

- *Creating an Authority-Based Group* on page 846
- *Deleting an Authority-Based Group* on page 848
- *Adding Authority-Based Users and Groups to Groups* on page 850
- *Removing Authority-Based Users or Groups from a Group* on page 852
- *Viewing or Modifying Authority-Based Group Options* on page 853
- *Generating Authority-Based Group DDL Commands* on page 854
- *Viewing or Modifying Authority-Based Group Properties* on page 855
- *Adding an Authority to a Group* on page 859
- *Removing an Authority from a Group* on page 861
- *Authority-Based Group Privilege Summary* on page 862
- *Authenticating a Login Account for a Managed Resource* on page 282

Adding Authority-Based Users and Groups to Groups

Add users and group to the current group or a higher-level parent group.

Prerequisites

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.

- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Groups**.
3. Select a group from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Members** or **Manage parent groups**
 - From the Administration Console menu bar, select **Resource > Manage Members** or **Resource > Manage parent groups**.

The Manage members of group or Manage parent groups view appears

4. To add members to the group or parent group, select one or more entries in the left-hand list and click **Add**.
 - The selected entries move to the right-hand list.
 - .

Tip: Use **Shift-click** or **Control-click** to select multiple entries.

5. Click **OK**.

See also

- *Creating an Authority-Based Group* on page 846
- *Deleting an Authority-Based Group* on page 848
- *Converting an Authority-Based Group to a User* on page 849
- *Removing Authority-Based Users or Groups from a Group* on page 852
- *Viewing or Modifying Authority-Based Group Options* on page 853
- *Generating Authority-Based Group DDL Commands* on page 854
- *Viewing or Modifying Authority-Based Group Properties* on page 855
- *Adding an Authority to a Group* on page 859
- *Removing an Authority from a Group* on page 861
- *Authority-Based Group Privilege Summary* on page 862
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing Authority-Based Users or Groups from a Group

Remove users and groups from the current group or a higher-level parent group.

Prerequisites

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Groups**.
3. Select a group from the right pane and either:
 - Click the arrow to the right of the name, or
 - From the Administration Console menu bar, select **Resource**.
4. To remove members from the group or parent group, select one or more entries in the right-hand list and click **Remove**.
The selected entries move to the left-hand list.
5. Click **OK**.

See also

- *Creating an Authority-Based Group* on page 846
- *Deleting an Authority-Based Group* on page 848
- *Converting an Authority-Based Group to a User* on page 849
- *Adding Authority-Based Users and Groups to Groups* on page 850
- *Viewing or Modifying Authority-Based Group Options* on page 853
- *Generating Authority-Based Group DDL Commands* on page 854
- *Viewing or Modifying Authority-Based Group Properties* on page 855
- *Adding an Authority to a Group* on page 859
- *Removing an Authority from a Group* on page 861
- *Authority-Based Group Privilege Summary* on page 862

- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Authority-Based Group Options

View or change database option settings assigned to a group.

Prerequisites

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

For database options that can be set at either level, when set at the user level, the setting overrides the current value for that user only. When set it at the database level, the value becomes the new default, and is applied to any existing users who have not had the option overridden at the user level.

For information on the level at each option can be set and the system privilege required, in the SAP Sybase IQ 15.x documentation, see the alphabetical list of Database options in *SAP Sybase IQ Reference: Statements and Options*.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Groups**.
3. Select a group from the right pane and either:
 - Click the arrow to the right of the name and select **Options**, or
 - From the Administration Console menu bar, select **Resource > Options**.

A list of the current settings of each option appears.

4. To change a setting, click in the Setting column for the option and enter the new value.
5. Choose one of the following:
 - Click **Apply** to save the change and continue modifying options.
 - Click **OK** to save all changes and close the Options view.

See also

- *Creating an Authority-Based Group* on page 846
- *Deleting an Authority-Based Group* on page 848
- *Converting an Authority-Based Group to a User* on page 849
- *Adding Authority-Based Users and Groups to Groups* on page 850
- *Removing Authority-Based Users or Groups from a Group* on page 852
- *Generating Authority-Based Group DDL Commands* on page 854
- *Viewing or Modifying Authority-Based Group Properties* on page 855
- *Adding an Authority to a Group* on page 859
- *Removing an Authority from a Group* on page 861
- *Authority-Based Group Privilege Summary* on page 862
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Authority-Based Group DDL Commands

Display the SQL data description language for creating a group. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Groups**.
3. Select one or more groups from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple groups.

The DDL view opens, showing the SQL code used to create the selected authority-based groups.

See also

- *Creating an Authority-Based Group* on page 846
- *Deleting an Authority-Based Group* on page 848
- *Converting an Authority-Based Group to a User* on page 849
- *Adding Authority-Based Users and Groups to Groups* on page 850
- *Removing Authority-Based Users or Groups from a Group* on page 852
- *Viewing or Modifying Authority-Based Group Options* on page 853
- *Viewing or Modifying Authority-Based Group Properties* on page 855
- *Adding an Authority to a Group* on page 859
- *Removing an Authority from a Group* on page 861
- *Authority-Based Group Privilege Summary* on page 862
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Authority-Based Group Properties

View or change the details of login parameters and authorities for a group.

Prerequisites

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	<p>View any property page – None required.</p> <p>Modify a password – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. • PERMS ADMIN authority. <p>Modify a login policy – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. <p>Modify any other group property except those relating to permissions –</p> <ul style="list-style-type: none"> • Requires DBA authority. <p>For privileges relating to group permissions, see:</p> <ul style="list-style-type: none"> • <i>Authority-Based Database Object Permissions Privilege Summary</i> on page 889
SAP Sybase IQ 16.0	Not supported

- The SAP Sybase IQ resource is authenticated and running.

- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Groups**.
3. Select a group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Group Properties view appears

4. View or edit the properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) Name of the user.</p> <p>Enable Password – Allows the user to connect to the database with password security. Clearing this option disables the Password and Confirm Password options.</p> <p>Password – The password for the user. Characters appear as asterisks.</p> <p>Confirm password – A field for confirming the password that you typed in the Password text box. The contents of the two fields must match exactly.</p> <p>Password creation time – Date and time when the password was created.</p> <p>Change password on next login – Force the user to change the password at the next login.</p> <p>Login policy – (Read-only) Select the login policy that applies for this user.</p> <p>Last login time – (Read-only) Last time the user successfully logged in.</p> <p>Failed login attempts – (Read-only) Number of times the user has tried to log in with an incorrect password.</p> <p>Locked – Displays false if the account is unlocked. Displays true if the user has exceeded the allowed number of failed login attempts.</p> <p>Unlock now –Unlocks the account if Locked is true.</p> <p>Comment – A text field for adding an optional comment about the user.</p>

Area	Description
Authorities	<p>Backup - Grants the ability to perform database backups.</p> <p>DBA - Grants the ability fully administer the database.</p> <p>Multiplex Admin - Grants the ability for Multiplex server administration.</p> <p>Operator - Grants the ability to backup and checkpoint databases, perform system monitoring, and drop connections.</p> <p>Perms Admin - Grants the ability to manage data permission, groups, authorities, and passwords.</p> <p>Profile - Grants the ability to perform application and procedure profiling, request log creation and analysis, and by the Index Consultant.</p> <p>Read client file - Grants the ability to read from a file on the client computer, for example when loading data.</p> <p>Read file - Grants the ability to the group to execute SELECT statements against a file using the OPENSTRING clause.</p> <p>Remote DBA - Grants Remote DBA authority to any table the group can access. To ensure that actions are secure, run the SQL Remote Message agent using a user ID with this type of authority.</p> <p>Resource - Grants the ability to create database objects.</p> <p>Space Admin - Grants the ability to perform dbspace management (including CREATE permission) and read-only selective database restoration.</p> <p>User Admin - Grants the ability to manage users, external logins, and login policies management.</p> <p>Validate - Grants the ability to validate tables, materialized views, and indexes.</p> <hr/> <p>Note: Materialized views are only supported for tables in the IQ system store.</p> <hr/> <p>Write client file - Grants the ability to write to a file on the client computer, for example when downloading data.</p>
Permission	See <i>Authority-Based User and Group Object Permissions</i> on page 865.

See also

- *Creating an Authority-Based Group* on page 846

- *Deleting an Authority-Based Group* on page 848
- *Converting an Authority-Based Group to a User* on page 849
- *Adding Authority-Based Users and Groups to Groups* on page 850
- *Removing Authority-Based Users or Groups from a Group* on page 852
- *Viewing or Modifying Authority-Based Group Options* on page 853
- *Generating Authority-Based Group DDL Commands* on page 854
- *Adding an Authority to a Group* on page 859
- *Removing an Authority from a Group* on page 861
- *Authority-Based Group Privilege Summary* on page 862
- *Authenticating a Login Account for a Managed Resource* on page 282

Adding an Authority to a Group

Add authorities to allow members of a group to perform specified database operations, such as the ability to manage dbspaces.

Prerequisites

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Groups**.
3. Select a group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Group Properties view appears

4. In the left pane, click **Authorities**.
5. In the right pane, select one or more authorities:

Authority	Description
Backup	Grants the ability to perform database backups.
DBA	Grants the ability fully administer the database.
Multiplex Admin	Grants the ability for Multiplex server administration
Operator	Grants the ability to backup and checkpoint databases, perform system monitoring, and drop connections.
Perms Admin	Grants the ability to manage data permission, groups, authorities, and passwords.
Profile	Grants the ability to perform application and procedure profiling, request log creation and analysis, and by the Index Consultant.
Read client file	Grants the ability to read from a file on the client computer, for example when loading data.
Read file	Grants the ability to the group to execute SELECT statements against a file using the OPENSTRING clause.
Remote DBA	Grants Remote DBA authority to any table the group can access. To ensure that actions are secure, run the SQL Remote Message agent using a user ID with this type of authority.
Resource	Grants the ability to create database objects.
Space Admin	Grants the ability to perform dbspace management (including CREATE permission) and read-only selective database restoration.
User Admin	Grants the ability to manage users, external logins, and login policies management.
Validate	Grants the ability to validate tables, materialized views, and indexes.
Write client file	Grants the ability to write to a file on the client computer, for example when downloading data.

6. Click **Apply** to save your changes and continue granting authorities, or click **OK** to save and close the properties view.

See also

- *Creating an Authority-Based Group* on page 846
- *Deleting an Authority-Based Group* on page 848
- *Converting an Authority-Based Group to a User* on page 849
- *Adding Authority-Based Users and Groups to Groups* on page 850

- *Removing Authority-Based Users or Groups from a Group* on page 852
- *Viewing or Modifying Authority-Based Group Options* on page 853
- *Generating Authority-Based Group DDL Commands* on page 854
- *Viewing or Modifying Authority-Based Group Properties* on page 855
- *Removing an Authority from a Group* on page 861
- *Authority-Based Group Privilege Summary* on page 862
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing an Authority from a Group

Remove a group's ability to perform specific authorized database operations.

Prerequisites

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based > Groups**.
3. Select a group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Group Properties view appears

4. In the left pane, click **Authorities**.
5. Clear the check box beside the authorities you want to revoke from the group.
6. Click **Apply** to save your changes and keep revoking authorities, or click **OK** to save and close the properties view.

See also

- *Creating an Authority-Based Group* on page 846
- *Deleting an Authority-Based Group* on page 848

- *Converting an Authority-Based Group to a User* on page 849
- *Adding Authority-Based Users and Groups to Groups* on page 850
- *Removing Authority-Based Users or Groups from a Group* on page 852
- *Viewing or Modifying Authority-Based Group Options* on page 853
- *Generating Authority-Based Group DDL Commands* on page 854
- *Viewing or Modifying Authority-Based Group Properties* on page 855
- *Adding an Authority to a Group* on page 859
- *Authority-Based Group Privilege Summary* on page 862
- *Authenticating a Login Account for a Managed Resource* on page 282

Authority-Based Group Privilege Summary

A list of the system privileges and object permissions required to complete the various authority-based group tasks.

Creating an Authority-Based Group

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• Both USER ADMIN and PERMS ADMIN authorities
SAP Sybase IQ 16.0	Not supported.

Deleting an Authority-Based Group

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• USER ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Converting an Authority-Based Group to a User

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Adding Authority-Based Users and Groups to Groups

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Removing Authority-Based Users and Groups from a Group

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Viewing or Modifying Authority-Based Group Options

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Generating Authority-Based Group DDL Commands

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	Not supported.

Viewing or Modifying Authority-Based Group Properties

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	<p>View any property page – None required.</p> <p>Modify a password – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. • PERMS ADMIN authority. <p>Modify a login policy – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority. <p>Modify any other group property except those relating to permissions –</p> <ul style="list-style-type: none"> • Requires DBA authority. <p>For privileges relating to group permissions, see:</p> <ul style="list-style-type: none"> • <i>Authority-Based Database Object Permissions Privilege Summary</i> on page 889
SAP Sybase IQ 16.0	Not supported

Granting or Revoking an Authority to a Group

Database Version	Authority-Based Group Permissions
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

See also

- *Creating an Authority-Based Group* on page 846
- *Deleting an Authority-Based Group* on page 848
- *Converting an Authority-Based Group to a User* on page 849
- *Adding Authority-Based Users and Groups to Groups* on page 850
- *Removing Authority-Based Users or Groups from a Group* on page 852
- *Viewing or Modifying Authority-Based Group Options* on page 853

- *Generating Authority-Based Group DDL Commands* on page 854
- *Viewing or Modifying Authority-Based Group Properties* on page 855
- *Adding an Authority to a Group* on page 859
- *Removing an Authority from a Group* on page 861

Authority-Based Object Permissions on Users and Groups

Permissions on database objects can be granted and revoked to users and groups, with or without administrative rights

Authority-Based Table and Column Permissions

Permissions on tables and columns can be granted and revoked to authority-based users and groups, with or without administrative rights.

About the User or Group Table Permissions List

The Tables permissions list displays permission details the tables and column directly granted to an authority-based user or group.

There are several table object permissions, which can be granted with or without administrative rights. Some permissions can be granted at the table level only, while others can be granted at either the table or column level.

- SELECT – table or column level
- INSERT – table level only
- DELETE – table level only
- UPDATE – table or column level
- ALTER – table level only
- REFERENCE – table or column level

These object permissions can be granted in several ways:

- You own the object.
- You are granted the DBA or PERMS ADMIN authority.
- You have been indirectly granted specific permissions through membership in a group to which permissions have been directly or indirectly granted.
- You have been directly granted specific permissions.

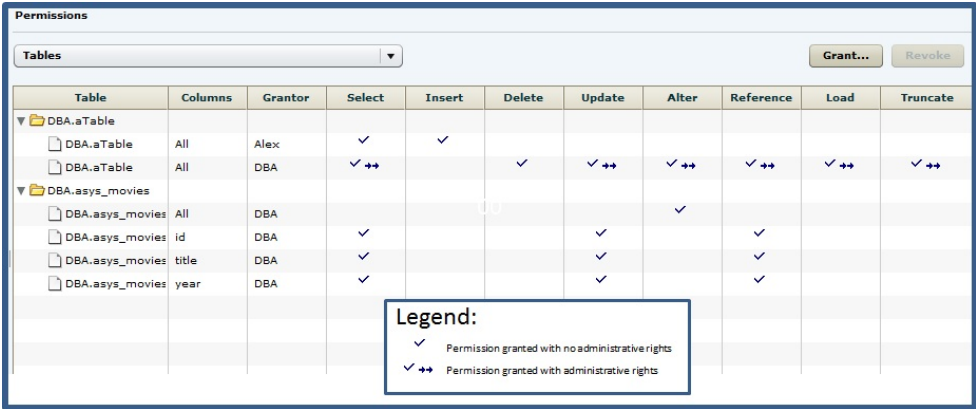
Users or groups with object ownership or the DBA or PERMS ADMIN authority are automatically granted all possible object permissions with administrative rights.

Object permissions can be granted with or without administrative rights. When granted without administrative rights, the grantee can perform authorized tasks requiring the permission, but cannot in turn grant the permission to another user or group. When granted with administrative rights (With grant option), the grantee can do both.

The permissions list only lists those tables or columns object permissions granted directly to the selected user or group. The list indicates the table and column the permission is granted on, by who (grantor), and the permissions and their corresponding administrative rights. The

permissions list does not list object permissions obtained through ownership, DBA or PERMS ADMIN authority, or group membership.

For each table, permissions granted to all columns on the table are listed first (all), followed by each column, sorted alphabetically by column name.



The screenshot shows the 'Permissions' window in SAP Sybase IQ. It features a table with columns: Table, Columns, Grantor, Select, Insert, Delete, Update, Alter, Reference, Load, and Truncate. The table lists permissions for various tables, including DBA.aTable and DBA.asys_movies. A legend box is overlaid on the table, explaining the symbols used for permissions.

Table	Columns	Grantor	Select	Insert	Delete	Update	Alter	Reference	Load	Truncate
DBA.aTable	All	Alex	✓	✓						
DBA.aTable	All	DBA	✓ ↔		✓	✓ ↔	✓ ↔	✓ ↔	✓ ↔	✓ ↔
DBA.asys_movies	All	DBA					✓			
DBA.asys_movies	id	DBA	✓			✓		✓		
DBA.asys_movies	title	DBA	✓			✓		✓		
DBA.asys_movies	year	DBA	✓			✓		✓		

Legend:
✓ Permission granted with no administrative rights
✓ ↔ Permission granted with administrative rights

When granted to a group, permissions, including administrative rights, are inherited by all members of the group. The group, not the users indirectly granted the permissions through inheritance, appear on the permissions list.

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or group.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the SELECT permission with the With grant option. UserA grants SELECT to UserB with the With grant option. UserB grants SELECT to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the SELECT permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

Permissions can be granted on the same table or column, by multiple grantors, resulting in the same table or column appearing multiple times on the list. If the same permission is granted to

the same table or column, with and without administrative rights, the grant with the administrative right takes precedence.

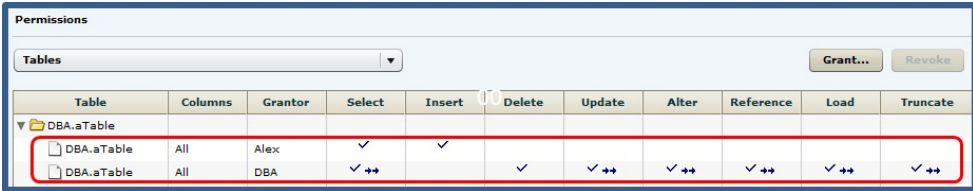


Table	Columns	Grantor	Select	Insert	Delete	Update	Alter	Reference	Load	Truncate
DBA.aTable	All	Alex	✓	✓						
DBA.aTable	All	DBA	✓ ++		✓	✓ ++	✓ ++	✓ ++	✓ ++	✓ ++

In this example, the user is granted the SELECT permission by both DBA and Alex, with different administrative rights. When the same permission is granted with different administrative rights, the higher administrative right takes precedence.

When revoking a permission granted multiple times, the permission is revoked from all instances, regardless of administrative rights. For example, Manager1 grants User2 INSERT with administrative rights. User1 also grants INSERT to User2, but without administrative rights. Regardless of which instance of INSERT is revoked, both instances of INSERT are revoked for User2.

Following the User or Group Table Permissions Grant Trail

Before revoking a grantee's permission, you need to identify grantees directly or indirectly granted the permission from the original grantee.

The grant chain traces how a grantee has in turn granted a permission to other grantees.

However, when you view the object permissions granted to a specific user, or group, you only see the permissions granted to the selected user or group. You do not see who the user or group has granted the permissions to.

To determine who the selected user or group has in turn granted an object permission to, note the table, column name (if applicable), and the permission to be traced, then display the permissions list for the table object to be traced. See *Setting Table Permissions > Following the Table Permissions Grant Trail* for details.

Adding Permissions on a Table or Column to a User or Group

Add permissions on a table or column to an authority-based user or group.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You have administrative rights (with grant option) to the permission.• You own the database object.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, click **Permissions**.
6. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
7. On the Welcome page, based on the table level to which permission is being granted, select **Tables** or **Table columns**.
8. Click **Next**.
9. Do one of:

Choice	Action
If Tables was selected	Select the table to apply permissions to. Click the box in the header row to select all available tables.
If Table Column was selected	<ul style="list-style-type: none"> Click the Table drop-down arrow and select the table containing the column to which permissions are to be applied. Select one or more columns to apply permissions to. Click the box in the header row to select all available columns on the table.

10. Click **Next**.

11. On the Permissions page, select one or more permissions. Click the box in the header row to select all available permissions.

12. (Optional) Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

13. Click **Finish**.

14. Click **OK**.

Note: To view the permissions granted on a table or column, click to expand the table name in the Table column.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Authority-Based Database Object Permissions Privilege Summary* on page 889

Removing Permissions on a Table or Column from a User or Group

Remove permissions on a table or column from an authority-based user or group.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> DBA authority. PERMS ADMIN authority. You have administrative rights (with grant option) to the permission. You own the database object.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.

- The selected resource supports authority-based security.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or group.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the SELECT permission with the With grant option. UserA grants SELECT to UserB with the With grant option. UserB grants SELECT to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the SELECT permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, click **Permissions**.
6. In the right pane, expand the table containing the permission to be revoked.
7. Highlight the row containing the permission to be modified.

Note: If the permission appears on the list multiple times with different grantors, with or without administrative rights, it does not matter which instance is selected.

8. Click **Revoke**.
A list of permissions currently granted (regardless of administrative rights) appears.
9. Select one or more permissions to revoke. Click the box in the header row to select all available permissions.

Warning! Revoking permissions may result in unexpected revocation from other users or groups. See *Following the User or Group Table Permission Grant Trail*.

10. Click **Finish**.

11. Click **OK**.

Note: The expanded table structure collapses, appearing as if all permissions were revoked, instead of the selected permission. Re-expand the table to view the remaining permissions.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Authority-Based Database Object Permissions Privilege Summary* on page 889

Removing Administrative Rights Only on a Table or Column Permission from a User or Group

Remove administrative rights only from a permission granted to an authority-based user or group, on a table or column.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.
- You are logged on as the original grantor of the permission with administrative rights to be removed.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes

precedence over any other non-administrative grants of the same permission to the same user or group.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, click **Permissions**.
6. In the right pane, click **Grant**.
7. On the Welcome page, based on the table level of the permission to be regranted, select **Tables** or **Table columns**.
8. Click **Next**.
9. On the Permissions page, select the permissions from which the administrative rights are being revoked.
10. Click **Finish**.
11. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Authority-Based Database Object Permissions Privilege Summary* on page 889

Adding Administrative Rights on a Granted Table or Column Permission to a User or Group

Add user or group administrative rights only to a granted table or column permission.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object.

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, click **Permissions**.
6. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
7. On the Welcome page, based on the table level of the existing permission to be granted administrative rights, select **Tables** or **Table columns**.
8. Click **Next**.
9. Do one of:

Choice	Action
If Tables was selected	Select the table containing the existing permission to which apply administrative rights are to be applied.
If Table Column was selected	<ul style="list-style-type: none"> • Click the Table drop-down arrow and select the table containing the column to which administrative rights are to be applied. • Select the columns containing the existing permission to which apply administrative rights are to be applied.

10. Click **Next**.
11. On the Permissions page, select the granted permissions to which administrative rights are to be granted.

12. Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

13. Click **Finish**.

14. Click **OK**.

Note: To view the permissions granted on a table or column, click to expand the table name in the Table column.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Authority-Based Database Object Permissions Privilege Summary* on page 889

Authority-Based View or Materialized View Permissions

Permissions on views and materialized view can be granted and revoked to authority-based users and groups, with or without administrative rights.

About the User or Group View Permissions List

The Views permissions list displays permission details the tables and column directly granted to an authority-based user or group.

There are four object permissions for views or materialized views, which can be granted with or without administrative rights:

- SELECT
- INSERT
- DELETE
- UPDATE

These object permissions can be granted in several ways:

- You own the object.
- You are granted the DBA or PERMS ADMIN authority.
- You have been indirectly granted specific permissions through membership in a group to which permissions have been directly or indirectly granted.
- You have been directly granted specific permissions.

Users or groups with object ownership or the DBA or PERMS ADMIN authority are automatically granted all possible object permissions with administrative rights.

Object permissions can be granted with or without administrative rights. When granted without administrative rights, the grantee can perform authorized tasks requiring the permission, but cannot in turn grant the permission to another user or group. When granted with administrative rights (With grant option), the grantee can do both.

The permissions list only lists those view and materialized view object permissions granted directly to the selected user or group. The list indicates the view or materialized view the

permission is granted on, by who (grantor), and the permissions and their corresponding administrative rights. The permissions list does not list object permissions obtained through ownership, DBA or PERMS ADMIN authority, or group membership.

The permissions list is sorted alphabetically by Grantor.

View	Grantor	Select	Insert	Delete	Update
DBA.cView	Alex	✓	✓ ↔	✓ ↔	
DBA.bView	DBA	✓ ↔		✓	✓ ↔

Legend:

✓ Permission granted with no administrative rights

✓ ↔ Permission granted with administrative rights

When granted to a group, permissions, including administrative rights, are inherited by all members of the group. The group, not the users indirectly granted the permissions through inheritance, appear on the permissions list.

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or group.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the SELECT permission with the With grant option. UserA grants SELECT to UserB with the With grant option. UserB grants SELECT to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the SELECT permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

Permissions can be granted on the same view or materialized view, by multiple grantors, resulting in the same view or materialized view appearing multiple times on the list. If the same permission is granted to the same view or materialized view, with and without administrative rights, the grant with the administrative right takes precedence.

View	Grantor	Select	Insert	Delete	Update
DBA.cView	Alex	✓ ↔	✓ ↔	✓ ↔	
DBA.bView	DBA	✓ ↔		✓	✓ ↔
DBA.cView	DBA	✓ ↔	✓		

When revoking a permission granted multiple times, the permission is revoked from all instances, regardless of administrative rights. For example, Manager1 grants User2 INSERT with administrative rights. User1 also grants INSERT to User2, but without administrative rights. Regardless of which instance of INSERT is revoked, both instances of INSERT are revoked for User2.

Following the User or Group View or Materialized View Permissions Grant Trail

Before revoking a grantee's permission, you need to identify grantees directly or indirectly granted the permission from the original grantee.

The grant chain traces how a grantee has in turn granted a permission to other grantees.

However, when you view the object permissions granted to a specific user, or group, you only see the permissions granted to the selected user or group. You do not see who the user or group has granted the permissions to.

To determine who the selected user or group has in turn granted an object permission to, note the table, column name (if applicable), and the permission to be traced, then display the permissions list for the table object to be traced. See *Setting View Permissions > Following the View Permissions Grant Trail* or *Setting Materialized View Permissions > Following the Materialized View Permissions Grant Trail* for details.

Adding Permissions on a View or Materialized View to a User or Group

Add permissions on a view or materialized view to an authority-based user or group.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> DBA authority. PERMS ADMIN authority. Administrative rights over the permission. You own the database object.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
 2. In the left pane, select **IQ Servers > Security > Authority Based**.
 3. Select:
 - **Users**
 - **Groups**
 4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
 5. In the left pane, click **Permissions**.
 6. Click the drop-down arrow and select **Views**.
A list of permissions currently granted to **Views** appears.
 7. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
 8. Select **Views**.
 9. Click **Next**.
 10. On the Objects page, select the view or materialized view on which the permission is being granted.
 11. Click **Next**.
 12. On the Permissions page, select one or more permissions. Click the box in the header row to select all available permissions.
 13. (Optional) Click the **With grant option** to grant the selected permissions administrative rights.
-
- Note:** The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.
-
14. Click **Finish**.
 15. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Authority-Based Database Object Permissions Privilege Summary* on page 889

Removing Permissions on a View or Materialized View from a User or Group

Remove permissions from a view or materialized view for an authority-based user or group.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• Administrative rights over the permission.• You own the database object.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or group.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the SELECT permission with the With grant option. UserA grants SELECT to UserB with the With grant option. UserB grants SELECT to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the SELECT permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, click **Permissions**.
6. Click the drop-down arrow and select **Views**.
A list of permissions currently granted to **Views** appears.
7. In the right pane, select the view or materialized view containing the permission to be revoked and click **Revoke**.
A list of permissions currently granted (regardless of administrative rights) appears.
8. Select one or more permissions to revoke. Click the box in the header row to select all available permissions.

Warning! Revoking permissions may result in unexpected revocation from other users or groups. See *Following the User or Group View Permission Grant Trail*.

9. Click **Finish**.
10. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Authority-Based Database Object Permissions Privilege Summary* on page 889

Removing Administrative Rights Only on a View or Materialized View Permission from a User or Group

Remove administrative rights only from a permission granted to an authority-based user or group, on a view or materialized view.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.
- You are logged on as the original grantor of the permission with administrative rights to be removed.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or group.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, click **Permissions**.
6. Click the drop-down arrow and select **Views**.
A list of permissions currently granted to **Views** appears.
7. In the right pane, click **Grant**.
8. Select **Views**.
9. Click **Next**.
10. On the Objects page, select the view or materialized view on which the administrative rights on a permissible are being removed.
11. Click **Next**.
12. On the Permissions page, select the permissions from which the administrative rights are being revoked.
13. Click **Finish**.

14. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Authority-Based Database Object Permissions Privilege Summary* on page 889

Adding Administrative Rights to a Granted View or Materialized View Permission to a User or Group

Add administrative rights only to a view or materialized view permission.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, click **Permissions**.
6. Click the drop-down arrow and select **Views**.
A list of permissions currently granted to views appears.
7. In the right pane, click **Grant**.

The Grant Permission Wizard appears.

8. Select **Views**.
 9. Click **Next**.
 10. On the Objects page, select the view or materialized view on which the existing permission to be granted administrative rights resides.
 11. Click **Next**.
 12. On the Permissions page, select the permission to which administrative rights are to be granted.
 13. Click the **With grant option** to grant the selected permissions administrative rights.
-
- Note:** The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.
-
14. Click **Finish**.
 15. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Authority-Based Database Object Permissions Privilege Summary* on page 889

Authority-Based Procedure or Function Permission

Grant and revoke execute permission on a function or procedure for an authority-based user or group

Adding EXECUTE Permission to a User or Group

Grant execute permission on a function or procedure to an authority-based user or group.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
 2. In the left pane, select **IQ Servers > Security > Authority Based**.
 3. Select:
 - **Users**
 - **Groups**
 4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
 5. In the left pane, select **Permissions**.
 6. Click the drop-down arrow and select **Procedures** or **Functions**.
A list of permissions currently granted to **Procedures** or **Functions** appears.
 7. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
 8. On the Welcome page, select **Procedures** or **Functions**.
 9. Click **Next**.
 10. On the Objects page, select one or more objects to grant execute permission to.
-
- Tip:** Use **Shift-click** or **Control-click** to select multiple objects.
-
11. Click **Next**.
 12. On the Permissions page, select **Execute**.
 13. Click **Finish**.
 14. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Authority-Based Database Object Permissions Privilege Summary* on page 889

Removing EXECUTE Permission from a User or Group

Remove execute permission on a function or procedure from an authority-based user or group.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. Click the drop-down arrow and select **Procedures** or **Functions**.
A list of permissions currently granted to **Procedures** or **Functions** appears.
7. In the right pane, highlight the permission to be revoked and click **Revoke**.
8. At the confirmation prompt, click **Yes**.
9. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Authority-Based Database Object Permissions Privilege Summary* on page 889

Authority-Based Dbspace Permission

Grant and revoke create permission on a dbspace for an authority-based user or group

Adding CREATE Permission to a User or Group

Add create permission on a dbspace to an authority-based user or group.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. Click the drop-down arrow and select **Dbspace**.
A list of permissions currently granted to **Dbspaces** appears.
7. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
8. On the Welcome page, select **Dbspaces**.
9. Click **Next**.
10. On the Objects page, select one or more objects to grant usage permission to.

Tip: Use **Shift-click** or **Control-click** to select multiple objects.

11. Click **Next**.
12. On the Permissions page, select **Create**.
13. Click **Finish**.
14. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Removing CREATE Permission from a User or Group

Remove create permission on a dbspace from an authority-based user or group.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. Click the drop-down arrow and select **Dbspace**.
A list of permissions currently granted to **Dbspaces** appears.

7. In the right pane, highlight the permission to be revoked and click **Revoke**.
8. At the confirmation prompt, click **Yes**.
9. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Authority-Based Sequence Generator Permission

Grant and revoke usage permission on a sequence generator for an authority-based user or group

Adding USAGE Permission to a User or Group

Add usage permission on a sequence generator to an authority-based user or group.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:
 - **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.

6. Click the drop-down arrow and select **Sequence Generator**.
A list of permissions currently granted to **Sequence Generators** appears.
7. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
8. On the Welcome page, select **Sequence Generators**.
9. Click **Next**.
10. On the Objects page, select one or more objects to grant usage permission to.

Tip: Use **Shift-click** or **Control-click** to select multiple objects.

11. Click **Next**.
12. On the Permissions page, select **Usage**.
13. Click **Finish**.
14. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Removing USAGE Permission from a User or Group

Remove usage permission on a sequence generator from an authority-based user or group.

Prerequisites

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the sequence generator.
SAP Sybase IQ 16.0	Not supported.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports authority-based security.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Authority Based**.
3. Select:

- **Users**
 - **Groups**
4. Select a user or group from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
 5. In the left pane, select **Permissions**.
 6. Click the drop-down arrow and select **Sequence Generators**.
A list of permissions currently granted to **Sequence Generators** appears.
 7. In the right pane, highlight the permission to be revoked and click **Revoke**.
 8. At the confirmation prompt, click **Yes**.
 9. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282

Authority-Based Database Object Permissions Privilege Summary

A list of the system privileges and object permissions required to complete the various authority-based user and group tasks pertaining to database objects.

Grant or Revoke Permissions on a Table or Column

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You have administrative rights (with grant option) to the permission. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

Modify Administrative Permissions on a Table or Column

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

Grant or Revoke Permissions on a View or Materialized View

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • Administrative rights over the permission. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

Modify Administrative Permissions on a View or Materialized View

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

Grant or Revoke Permissions on a Sequence Generator

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the sequence generator.
SAP Sybase IQ 16.0	Not supported.

Grant or Revoke Permissions on a Function or Procedure

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Not supported.

Grant or Revoke Permissions on a Dbspace

Database Version	Authority-Based Database Object Permissions
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Not supported.

Role-Based Security

Add, change, and delete users and roles and grant or revoke database system roles to same.

Role-based security is supported with database version 16.0 only.

Role Types

In role-based security, there are several types of roles.

- **User-defined Role** – can be granted privileges on other objects. Membership to a user-defined role can be granted to users or other user-defined roles. User-defined roles include:
 - **Standalone role** – an independent database object without login privileges, which can own objects. You cannot convert a standalone role to a user-extended role, and vice versa.
 - **User-extended role** – a user ID that has been extended to act as a role. If an original user has login privileges, a user-extended role inherits the login privileges.
- **System roles** – are automatically created in each newly created or upgraded database and are granted specific system privileges. System roles cannot be dropped and cannot own objects. They do not follow any specific naming conventions.
- **Compatibility Roles** – are automatically created in each newly created or upgraded database and are granted specific system roles and privileges. Compatibility roles can be migrated and dropped under specific conditions and use a naming convention that begin

with SYS_AUTH_ and end with _ROLE. Also called predefined roles, they are created for backward compatibility with earlier versions of SAP Sybase IQ.

Role-Based Users

Add, change, and delete role-based users.

See also

- *Configuring SAP Sybase IQ Roles-Based Users for Monitoring* on page 129

Creating a Role-Based User

Add a new role-based user to the database using the Create User wizard.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Creating a user requires MANAGE ANY USER system privilege.</p> <p>Granting a role during the user creation process requires one of:</p> <ul style="list-style-type: none">• Administrative rights over the role being granted (role administrator).• MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>Granting a system privilege during user creation requires administrative rights over the system privilege being granted.</p>

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Click the arrow next to **Users** and select **New**.
The Create User Wizard appears.
4. On the Welcome page, specify

Option	Description
Select a resource on which the user will be created.	Select a resource from the list.
	Note: If the selected resource does not support role-based security, an error message appears.
What do you want to name the new user?	Enter a unique user ID.

5. Click Next.
6. On the Password page:

Option	Description
Enable password	Select to allow a user to connect to the database with password security. Leave this option unselected to disable the password and confirm password options.
Password	Create a strong user password. Characters appear as asterisks.
Confirm password	Confirms the password. The contents of the two password fields must match exactly.
Requires password change on next login	Select to force a user to change his or her password at the next login. Note: This functionality is not currently implemented in Sybase Control Center. When logging in to Sybase Control Center, a user will not be prompted to change their password. He or she will be prompted, however, when logging in to SAP Sybase IQ outside of Sybase Control Center (for example, using Interactive SQL).
Login policy	Select a login policy from the list.

7. Click Next.
8. On the Roles page, highlight a role to be granted. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

- Only roles to which you have administrative rights appear on the list.
- By default, a new user or user-extended role is automatically granted the PUBLIC system role with the "Role only" privilege (user is a member of the role, but has no administrative rights on the role). There is no need to add the PUBLIC role when creating a user, user-extended role, or standalone role.
- When you grant a role to a user, user-extended role, or standalone role, unless otherwise noted, any underlying system privileges of the role being granted are automatically inherited by the user, user-extended role, or standalone role.

9. Repeat step 8 to grant additional roles.

10. Click **Next**.

11. On the System Privileges page, highlight a system privilege to be granted. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Note: Only system privileges to which you have administrative rights appear on the list.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

12. Repeat step 11 to grant additional privileges.

13. Click **Next**.

14. (Optional) On the Comment page, enter a comment for this user.

15. Click **Finish**.

See also

- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907

- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Role-Based User

Delete a role-based user from the database.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security
- The user being deleted does not own any database objects and is not currently connected to the database.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select one or more users from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple users.

4. Click **Yes** to confirm deletion.

See also

- *Creating a Role-Based User* on page 892
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897

- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Converting a Role-Based User to a User-Extended Role

Change an existing user to act as a role. The user-extended role retains membership roles already granted to the user.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Change to Role**, or
 - From the Administration Console menu bar, select **Resource > Change to Role**.
4. Click **Yes** to confirm conversion.

After converting the user, if any of the following roles were granted to the original user, the underlying system privileges and roles are automatically inherited by any users added to the

role. This can be prevented, for these roles only, by changing the administrative rights on the role along with the no inheritance option.

- SYS_AUTH_DBA_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_RUN_REPLICATION_ROLE
- SYS_AUTH_RESOURCE_ROLE
- SYS_AUTH_VALIDATE_ROLE

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936

Adding a Role to a Role-Based User

Add a role-based user a member of a role. The user inherits all underlying system privileges and roles of the granted role.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based User Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

A list of roles currently granted to the user appears.

4. Click **Grant**.
5. Select one or more roles to grant. Only roles to which you have administrative rights appear on the list.

Tip: Use **Shift-click** or **Control-click** to select multiple roles.

6. Click **OK** to grant the roles.
The selected roles appear with **Role only** rights (no administrative rights).
7. (Optional) To modify the administrative rights of a role, highlight a role. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

8. Click **OK**.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing a Role-Based User's Administrative Rights on a Role

Change a role-based user's ability to manage a role.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • Administrative rights over the role (role administrator). • MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Security > Role-Based > Users** .
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

A list of roles currently granted and their administrative rights appears.

4. Highlight a role to be modified. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

5. Click **OK**.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing a Role from a Role-Based User

Remove a role-based user's membership in a role.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

By default, a minimum of one role administrator (or global role administrator with a login password) for each role must exist at all times. This minimum requirement is validated before you can remove a member who is a role administrator from a role.

If removing membership in a role would result in a failure to meet the minimum number of role administrators for the selected role, an error message appears, and the task fails.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

A list of roles currently granted to the user appears.

4. Highlight a role to be removed and click **Revoke**.

Note: The **Revoke** button is unavailable if you do not have administrative rights to the selected role.

5. Click **OK**.

See also

- *Creating a Role-Based User* on page 892

- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Adding a System Privilege to a Role-Based User

Allows a role-based user to perform privileged tasks associated with a system privilege.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the user appears.

4. Click **Grant**.
5. Select one or more system privileges to grant. Only system privileges to which you have administrative rights appear on the list.

Tip: Use **Shift-click** or **Control-click** to select multiple system privilege.

6. Click **OK** to grant the system privileges.
The selected system privileges appear granted with **Privilege only** rights (no administrative rights).
7. (Optional) To modify the administrative rights of a system privilege, highlight a system privilege. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

8. Click **OK**.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914

- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing a User's Administrative Rights on a System Privilege

Changes a user's ability to manage a system privilege.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the user appears.

4. Highlight a system privilege to be modified. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.

Grant Option	Description
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

5. Click **OK**.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing a System Privilege from a Role-Based User

Remove a system privilege from a role-based user.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the user appears.

4. Highlight a system privilege to be removed and click **Revoke**.

Note: The **Revoke** button is unavailable if you do not have administrative rights to the selected system privilege.

5. Click **OK**.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Role-Based User Options

View or change database option settings assigned to a user.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	<p>View the list of options – None required.</p> <p>Modify any option – Depending on the option being modified, requires one of these:</p> <ul style="list-style-type: none"> • SET ANY PUBLIC OPTION system privilege. • SET ANY SECURITY OPTION system privilege. • SET ANY SYSTEM OPTION system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

For database options that can be set at either level, when set at the user level, the setting overrides the current value for that user only. When set it at the database level, the value becomes the new default, and is applied to any existing users who have not had the option overridden at the user level.

For information on the level at each option can be set and the system privilege required, in the SAP Sybase IQ 16.x documentation, see the alphabetical list of Database options in *SAP Sybase IQ Reference: Building Blocks, Tables, and Procedures*.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Options**, or
 - From the Administration Console menu bar, select **Resource > Options**.

A list of the current setting for each option appears.

4. To change a setting, click in the Setting column of the option and enter the new value.
5. Choose one of the following:

- Click **Apply** to save the change and continue modifying options.
- Click **OK** to save all changes and close the Options view.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Role-Based User DDL Commands

Display the SQL data description language for creating a user. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select one or more users from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple users.

The DDL view opens, showing the SQL code used to create the selected role-based users.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Role-Based User Properties

View or change user properties such as password, login policy and database object permissions.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.

Database Version	Role-Based User Privileges
SAP Sybase IQ 16.0	<p>View any user property page – None required.</p> <p>Modify a password – Requires CHANGE PASSWORD system privilege.</p> <p>Modify a login policy, comment, or refresh DN – Requires MANAGE ANY USER system privilege.</p> <p>Refresh LDAP DN - Requires MANAGE ANY USER system privilege.</p> <p>For privileges relating to user permissions, see:</p> <ul style="list-style-type: none"> • <i>Role-Based Database Object Permissions Privilege Summary</i> on page 1034

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties view appears

4. View or edit the properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read only) Name of the user.</p> <p>Enable Password – Allows the user to connect to the database with password security. Clearing this option disables the Password and Confirm Password options.</p> <p>Password – The password for the user. Characters appear as asterisks.</p> <p>Confirm password – A field for confirming the password that you typed in the Password text box. The contents of the two fields must match exactly.</p> <p>Password creation time – Date and time when the password was created.</p> <p>Change password on next login – Select to force the user to change the password at the next login.</p> <hr/> <p>Note: This functionality is not currently implemented in Sybase Control Center. When logging in to Sybase Control Center, a user will not be prompted to change their password. He or she will be prompted, however, when logging in to SAP Sybase IQ outside of Sybase Control Center (for example, using Interactive SQL).</p> <hr/> <p>Login policy – Select a login policy for the user from the list.</p> <p>Last login time – Last time the user successfully logged in.</p> <p>Failed login attempts – Number of times the user has tried to log in with an incorrect password.</p> <p>Locked – Displays false if the account is unlocked. Displays true if the user has exceeded the allowed number of failed login attempts.</p> <p>Unlock now – Unlocks the account if Locked is true.</p> <p>Comment – A text field for adding an optional comment about the user.</p>
LDAP	Refresh the user DN.
Permission	See <i>Role-Based User and Role Object Permissions</i> on page 1008.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899

- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing a Role-Based User Password

Change the password for another role-base user.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires CHANGE PASSWORD system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties page appears.

4. On the General Properties page, type the new password in the Password and Confirm password fields.
5. Click **OK**.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Forcing a Role-Based User to Change their Password

Force a role-based user to change their password the next time he or she logs in.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

This functionality is not currently implemented in Sybase Control Center. When logging in to Sybase Control Center, a user will not be prompted to change their password. He or she will be prompted, however, when logging in to SAP Sybase IQ outside of Sybase Control Center (for example, using Interactive SQL).

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties page appears.

4. On the General Properties page, select **Require password change on next login**.
5. Click **OK**.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Unlocking a Role-Based User Account

Unlock a locked role-based user account.

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

- The SAP Sybase IQ resource is authenticated and running.

- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties page appears.

4. On the General Properties page, click **Unlock Now**.
5. Click **OK**.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Changing a Role-Based User Login Policy* on page 916
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing a Role-Based User Login Policy

Assign a role-based user a different login policy

Prerequisites

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Users**.
3. Select a user from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User Properties page appears.

4. Select a new login policy from the list.
5. Click **OK**.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909

- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Role-Based User Privilege Summary* on page 917
- *Authenticating a Login Account for a Managed Resource* on page 282

Role-Based User Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based user tasks.

Creating a Role-Based User

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Creating a user requires MANAGE ANY USER system privilege.</p> <p>Granting a role during the user creation process requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the role being granted (role administrator). • MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>Granting a system privilege during user creation requires administrative rights over the system privilege being granted.</p>

Deleting a Role-Based User

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Converting a Role-Based User to a User Extended Role

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege.

Adding and Removing a User from a Role

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

Adding and Removing System Privileges from a User

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege.

Viewing or Modifying Role-Based User Options

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	View the list of options – None required. Modify any option – Depending on the option being modified, requires one of these: <ul style="list-style-type: none"> SET ANY PUBLIC OPTION system privilege. SET ANY SECURITY OPTION system privilege. SET ANY SYSTEM OPTION system privilege.

Generating Role-Based User DDL Commands

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Role-Based User Properties

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	<p>View any user property page – None required.</p> <p>Modify a password – Requires CHANGE PASSWORD system privilege.</p> <p>Modify a login policy, comment, or refresh DN – Requires MANAGE ANY USER system privilege.</p> <p>Refresh LDAP DN - Requires MANAGE ANY USER system privilege.</p> <p>For privileges relating to user permissions, see:</p> <ul style="list-style-type: none"> • <i>Role-Based Database Object Permissions Privilege Summary</i> on page 1034

Changing a Role-Based User Password

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Forcing a Role-Based User Password Change

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires CHANGE PASSWORD system privilege.

Unlocking a Role-Based User Account

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Changing a Role-Based User Login Policy

Database Version	Role-Based User Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

See also

- *Creating a Role-Based User* on page 892
- *Deleting a Role-Based User* on page 895
- *Converting a Role-Based User to a User-Extended Role* on page 896
- *Adding a Role to a Role-Based User* on page 897
- *Changing a Role-Based User's Administrative Rights on a Role* on page 899
- *Removing a Role from a Role-Based User* on page 901
- *Adding a System Privilege to a Role-Based User* on page 902
- *Changing a User's Administrative Rights on a System Privilege* on page 904
- *Removing a System Privilege from a Role-Based User* on page 905
- *Viewing or Modifying Role-Based User Options* on page 907
- *Generating Role-Based User DDL Commands* on page 908
- *Viewing or Modifying Role-Based User Properties* on page 909
- *Changing a Role-Based User Password* on page 912
- *Forcing a Role-Based User to Change their Password* on page 913
- *Unlocking a Role-Based User Account* on page 914
- *Changing a Role-Based User Login Policy* on page 916

Security Implications of the Managing Grantees and Managing Roles Options

A role can be granted to another role as a grantee (member) or as an underlying role. Each grant type has different security inheritance implications.

Grantees are members granted directly to a role. A grantee can be either a user or another role. Granting membership in a role allows grantees to inherit all system privileges and underlying roles of the role.

When granting a role to another role, the role can be granted as a grantee (member)) or as an underlying role.

When a role is granted as a member, each member of the role being granted (the child role) becomes a grantee of the receiving role (the parent role). Each new grantee inherits all system privileges and roles already granted to the parent role, while still retaining all system privileges and roles from the child role. Existing members of the parent role do not inherit any system privileges and roles from the child role.

When a role is granted as an underlying role, all system privileges and roles of the underlying role (child role) are inherited by all members of the receiving role (parent role). However, members of the child role do not become members of the parent role.

Consider the following:

- There are three users: User1, User2, User3.
- There are five roles: Role1, Role2, Role3, Role4, Role5.
- There are three system privileges: Priv1, Priv2, Priv3.

Grant a role as a member:

- Role1 is granted Priv1 and Role4.
- User1 and User2 are members of Role1.
- Role2 is granted Priv2 and Role5.
- User3 is a member of Role2.
- Role1 is made a member of Role2 (**Manage Grantee**).
- As members of Role1, User1 and User2 (indirectly) become members of Role2 and inherit Priv2. Since Role4 is also a member of Role1, they also (indirectly) inherit all system privileges and roles granted to Role4.
- As a member of Role2, User3 does not inherit Priv1 from Role1, or any system privileges or roles of Role4.

Grant a role as an underlying role:

- Role1 is granted Priv1 and Role4.
- User1 and User2 are members of Role1.
- Role2 is granted Priv2 and Role5.
- User3 is a member of Role2.
- Role1 is made an underlying role of Role2 (**Manage Roles**).
- As a member of Role2, User3 inherits the following from Role1: Priv1 and (indirectly) all system privileges and roles of Role4.
- As members of Role1, User1 and User2 do not become members of Role2 and do not inherit Priv2 or any system privileges and roles granted to Role4.

As you can see, there is a significant difference in how system privileges and roles of a child role are inherited by the parent role and by whom. Use of the wrong grant method can lead to unexpected behavior and potential security concerns.

User-Extended Roles

Add, change, and delete user-extended roles.

Creating a User-Extended Role

Add a new user-extended role to the database.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Creating a role requires both the MANAGE ANY USER and MANAGE ROLES system privileges.</p> <p>Granting a role during user-extended role creation requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role being granted (role administrator). MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>Granting a system privilege during user-extended role creation requires administrative rights over the system privilege being granted.</p>

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Click the arrow next to **User-Extended Roles** and select **New**.
The Create User-Extended Role Wizard appears.
4. On the Welcome page, specify

Option	Description
Select a resource on which the user will be created.	<p>Select a resource from the list.</p> <hr/> <p>Note: If the selected resource does not support role-based security, an error message appears.</p>
What do you want to name the new user?	Enter a unique user ID.

5. Click **Next**.

6. On the Password page:

Option	Description
Enable password	Select to allow a user to connect to the database with password security. Leave this option unselected to disable the password and confirm password options.
Password	Create a strong user password. Characters appear as asterisks.
Confirm password	Confirms the password. The contents of the two password fields must match exactly.
Requires password change on next login	Select to force a user to change his or her password at the next login. Note: This functionality is not currently implemented in Sybase Control Center. When logging in to Sybase Control Center, a user will not be prompted to change their password. He or she will be prompted, however, when logging in to SAP Sybase IQ outside of Sybase Control Center (for example, using Interactive SQL).
Login policy	Select a login policy from the list.

7. Click **Next**.

8. On the Administrators page, select one or more administrators.

Note: It is strongly recommended that you do not select any role administrators when creating a new role; add them once the creation process is complete. If at least one role administrator is specified during creation, global role administrators will be unable to manage the role because the MANAGE ROLES system privilege is not automatically granted to the role.

9. If an administrator is selected, indicate whether the administrator is to be granted membership in the role along with administrative rights (Administrative and role) or administrative rights only (default).

Note: Only one privilege level can be defined for all selected administrators when specified during the create process. However, the privilege level can be later modified. See *Manage User-Extended Role Administrators*

10. Click **Next**.

11. On the Roles page, highlight a role to be granted. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.

Grant Option	Description
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

- Only roles to which you have administrative rights appear on the list.
- By default, a new user or user-extended role is automatically granted the PUBLIC system role with the "Role only" privilege (user is a member of the role, but has no administrative rights on the role). There is no need to add the PUBLIC role when creating a user, user-extended role, or standalone role.
- When you grant a role to a user, user-extended role, or standalone role, unless otherwise noted, any underlying system privileges of the role being granted are automatically inherited by the user, user-extended role, or standalone role.

12. Repeat step 11 to grant additional roles.

13. Click **Next**.

14. On the System Privileges page, highlight a system privilege to be granted. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Note: Only system privileges to which you have administrative rights appear on the list.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

15. Repeat step 14 to grant additional privileges.

16. Click **Next**.

17. (Optional) On the Comment page, enter a comment for this user.

18. Click **Finish**.

See also

- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927

- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a User-Extended Role

Delete a user-extended role from the database.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security
- The user-extended role being deleted does not own any database objects and is not currently connected to the database.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select one or more roles from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple user-extended roles.

4. Click **Yes** to confirm deletion.

See also

- *Creating a User-Extended Role* on page 922
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Converting a User-Extended Role to a User

Change a user-extended role back to a regular user.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the role being converted.

Task

The user retains any login privileges, system privileges and roles granted to the user-extended role. The user remains as the owner of the objects that were created after the user was extended to act as a role. Any users granted to the user-extended role are immediately revoked.

A minimum number of role or global role administrators (as defined by the **MIN_ROLE_ADMINS** database option) with a login password must exist for each role at all times. When converting a user-extended role back to a user, all dependent roles of the user-extended role must continue to meet this minimum requirement, or the conversion fails.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a role from the right pane and either:
 - Click the arrow to the right of the name and select **Change to User**, or
 - From the Administration Console menu bar, select **Resource > Change to User**.
4. Click **Yes** to confirm conversion.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941

- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Adding a Grantee to a User-Extended Role

Add a user or role as a member (grantee) of a user-extended role. Grantee inherits all underlying system privileges and roles of the user-extended role.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• Administrative rights over the role (role administrator).• MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or

- From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When adding a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the role appears.

- Click **Grant**.
- Select one or more users or roles to become members. Only roles to which you have administrative rights appear on the list.

Tip: Use **Shift-click** or **Control-click** to select multiple roles.

- Click **OK**.
The new grantees appear with **Role only** rights (no administrative rights).
- (Optional) To modify the administrative rights of a role, highlight a role. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

- Click **OK**.

See also

- Creating a User-Extended Role* on page 922
- Deleting a User-Extended Role* on page 925
- Converting a User-Extended Role to a User* on page 927
- Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- Removing a Grantee From a User-Extended Role* on page 932
- Adding a Role to a User-Extended Role* on page 933
- Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- Removing a Role from a User-Extended Role* on page 939
- Adding a System Privilege to a User-Extended Role* on page 941
- Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- Removing a System Privilege from a User-Extended Role* on page 944

- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Changing a Grantee's Administrative Rights on a User-Extended Role

Change a member's (grantee's) ability to manage a user-extended role.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• Administrative rights over the role (role administrator).• MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When modifying the administrative rights of a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance

outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the role appears.

4. Highlight a user or role to be modified. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

5. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965

- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Removing a Grantee From a User-Extended Role

Remove a user or role as a member (grantee) of a user-extended role. Grantees lose the ability to use any underlying system privileges or roles of the user-extended role.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• Administrative rights over the role (role administrator).• MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

By default, a minimum of one role administrator (or global role administrator with a login password) for each role must exist at all times. This minimum requirement is validated before you can remove a member who is a role administrator from a role.

If revoking membership in a role would result in a failure to meet the minimum number of role administrators for the selected role, an error message appears, and the removal fails.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When removing a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the role appears.

4. Highlight a user or role to be removed from the user-extended role and click **Revoke**.

Note: The **Revoke** button is unavailable if you do not have administrative rights to the selected role.

5. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Adding a Role to a User-Extended Role

Add a role as an underlying role of a user-extended role. Members of the user-extended role inherit all system privileges and roles of the underlying role, but do not become members of

the underlying role. Members of the underlying role do not become members of the user-extended role.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none">• Administrative rights over the role (role administrator).• MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none">• Administrative rights over the underlying role (role administrator).• MANAGE ROLES system privilege if the underlying role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

Warning! When adding an underlying role to a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of roles currently granted to the user-extended role appears.

4. Click **Grant**.

5. Select one or more system or compatibility roles to grant. Only roles to which you have administrative rights appear on the list.

Tip: Use **Shift-click** or **Control-click** to select multiple roles.

6. Click **OK**.

The selected roles appear with **Role only** rights (no administrative rights).

7. (Optional) (For compatibility and user-defined roles only) To modify the administrative rights of an underlying role, highlight a role. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

Note: The following steps represent a behavior change with SAP Sybase IQ 16.0, for the following roles only.

- SYS_AUTH_DBA_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_RUN_REPLICATION_ROLE
- SYS_AUTH_RESOURCE_ROLE
- SYS_AUTH_VALIDATE_ROLE

Prior to 16.0, when granting membership to one of these roles, the default inheritance behavior was to not allow members of the role to automatically inherit the underlying system privileges and roles of the compatibility role. Only the log on user (of the role) would inherit. As of 16.0, the default behavior is to allow automatic inheritance by all members of the role.

8. (Optional for SYS_AUTH_DBA_ROLE only) To prevent automatic inheritance of the SYS_AUTH_DBA_ROLE when granted with the **Administrative and Role** option, click in the Inheritance column, and select No Inheritance.
9. (Optional for SYS_AUTH_DBA_ROLE, SYS_AUTH_BACKUP_ROLE, SYS_RUN_REPLICATION_ROLE, SYS_AUTH_RESOURCE_ROLE, or SYS_AUTH_VALIDATE_ROLE only) To prevent automatic inheritance when granted with **Role only** option, click in the Inheritance column, and select No Inheritance.
10. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922

- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Changing Administrative Rights on an Underlying Role of a User-Extended Role

Changes a member's (grantee's) ability to manage an underlying role of a user-extended role.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • Administrative rights over the role (role administrator). • MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

Administrative rights cannot be modified on underlying system roles.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Role**.
3. Select a user-extended role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

Warning! When modifying the administrative rights of an underlying role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of underlying roles currently granted to the role appears.

4. (Not applicable to system roles) Highlight a role to be modified. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

Note: The following steps represent a behavior change with SAP Sybase IQ 16.0, for the following roles only.

- SYS_AUTH_DBA_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_RUN_REPLICATION_ROLE
- SYS_AUTH_RESOURCE_ROLE
- SYS_AUTH_VALIDATE_ROLE

Prior to 16.0, when granting membership to one of these roles, the default inheritance behavior was to not allow members of the role to automatically inherit the underlying system privileges and roles of the compatibility role. Only the log on user (of the role)

would inherit. As of 16.0, the default behavior is to allow automatic inheritance by all members of the role.

5. (Optional for SYS_AUTH_DBA_ROLE only) To prevent automatic inheritance of the SYS_AUTH_DBA_ROLE when granted with the **Administrative and Role** option, click in the Inheritance column, and select No Inheritance.
6. (Optional for SYS_AUTH_DBA_ROLE, SYS_AUTH_BACKUP_ROLE, SYS_RUN_REPLICATION_ROLE, SYS_AUTH_RESOURCE_ROLE, or SYS_AUTH_VALIDATE_ROLE only) To prevent automatic inheritance when granted with **Role only** option, click in the Inheritance column, and select No Inheritance.
7. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Removing a Role from a User-Extended Role

Remove a role as an underlying role of a user-extended role. Members of the user-extended role lose the ability to use any system privileges of the underlying role.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a user-extended role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

Warning! When removing an underlying role from a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of underlying roles currently granted to the user-extended role appears.

4. Highlight a role to be removed and click **Revoke**.

Note: The **Revoke** button is unavailable if you do not have administrative rights to the selected role.

5. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Adding a System Privilege to a User-Extended Role

Add the ability of a user-extended role to perform privileged tasks associated with a system privilege.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a user-extended role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the user-extended role appears.

4. Click **Grant**.
5. Select one or more system privileges to grant. Only system privileges to which you have administrative rights appear on the list.

Tip: Use **Shift-click** or **Control-click** to select multiple system privilege.

6. Click **OK** to grant the system privilege.
The selected system privileges appear granted with **Privilege only** rights (no administrative rights).
7. (Optional) To modify the administrative rights of a system privilege, highlight a system privilege. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

8. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing Administrative Rights on a User-Extended Role Granted Privilege

Change the administrative rights on a system privilege granted to a user-extended role.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a user-extended role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the user-extended role appears.

4. Highlight a system privilege to be modified. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

5. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing a System Privilege from a User-Extended Role

Remove a system privilege from a user-extended role.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a user-extended role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the user-extended role appears.

4. Highlight a system privilege and click **Revoke**.

Note: The **Revoke** button is unavailable if you do not have administrative rights to the selected system privilege.

5. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965

- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Role-Based User-Extended Role Options

View or change database option settings assigned to a user.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	<p>View user-extended role options only – None required.</p> <p>Modify user-extended role options – Depending on the option being modified, requires one of these:</p> <ul style="list-style-type: none">• SET ANY PUBLIC OPTION system privilege.• SET ANY SECURITY OPTION system privilege.• SET ANY SYSTEM OPTION system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

For database options that can be set at either level, when set at the user level, the setting overrides the current value for that user only. When set it at the database level, the value becomes the new default, and is applied to any existing users who have not had the option overridden at the user level.

For information on the level at each option can be set and the system privilege required, in the SAP Sybase IQ 16.x documentation, see the alphabetical list of Database options in *SAP Sybase IQ Reference: Building Blocks, Tables, and Procedures*.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a user-extended role from the right pane and either:
 - Click the arrow to the right of the name and select **Options**, or
 - From the Administration Console menu bar, select **Resource > Options**.

A list of the current settings of each option appears.

4. To change a setting, click in the Setting column for the option and enter the new value.

5. Choose one of the following:

- Click **Apply** to save the change and continue modifying options.
- Click **OK** to save all changes and close the Options view.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Manage Role Administrators of a User-Extended Role

Role administrators are responsible for granting and revoking user-extended roles to users and other roles. You can add and remove role administrators as needed.

There are two types of role administrators:

- Role administrator – users or roles designated to administer a role.
- Global role administrator – any user granted the MANAGE ROLES system privilege.

When you create a new role, you can appoint one or more role administrators to manage the role (grant and revoke membership in the role). If no role administrator is specified during the creation process, the MANAGE ROLES system privilege is automatically granted to the role

with the Administrative Only privilege, which creates the global role administrator for a role. However, if at least one administrator is specified during the creation process, the **MANAGE ROLES** system privilege is not granted to the role and global role administrators will be unable to manage the role. For this reason, it is recommended that role administrators not be specified when creating a new role. They should be added after the fact. This ensures that every role can be successfully managed by both role and global role administrators.

A role administrator can add or remove other role administrators from a role, including global role administrators. Both role administrators and global role administrators can grant, revoke, and drop roles. A role administrator does not require the **MANAGE ROLES** system privilege to administer a role.

By default, at least one role administrator or global role administrator with a login password must exist at all times for each role. This minimum requirement is validated before you can remove the global role administrator or role administrator from a role, or remove a role administrator's administrative rights on a role. The minimum requirement is a configurable database option (**MIN_ROLE_ADMINS**).

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966

Adding a Role Administrator to an Existing User-Extended Role

Add a new role administrator to an existing user-extended role.

Prerequisites

Database Version	Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role being managed. MANAGE ROLES system privilege if the role being granted has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a role from the right pane and do one of:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When adding a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users or roles currently granted to the role appears. Any user or role with **Administrative only** or **Administrative and role** in the Grant Option column is a role administrator.

4. Click **Grant**.
5. Select one or more users or roles. Only roles to which you have administrative rights appear on the list.

Tip: Use **Shift-click** or **Control-click** to select multiple users or roles.

6. Click **OK** to grant membership.
The selected users or roles appear with **Role only** rights (no administrative rights).

7. For each new administrator added, click in the Grant Options column, click the arrow, and select:

Grant Option	Description
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

8. Click **OK**.

See also

- *Removing a Role Administrator from a User-Extended Role* on page 950
- *Modifying a User-Extended Role Administrator's Administrative Rights* on page 951
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing a Role Administrator from a User-Extended Role

Remove a role administrator from an existing user-extended role.

Prerequisites

Database Version	Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • Administrative rights over the role being managed. • MANAGE ROLES system privilege if the role being granted has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

By default, at least one role administrator or global role administrator with a login password must exist at all times for each role. This minimum requirement is validated before you can remove the global role administrator or role administrator from a role, or remove a role administrator's administrative rights on a role. The minimum requirement is a configurable database option (**MIN_ROLE_ADMINS**).

If revoking membership in a role would result in a failure to meet the minimum number of role administrators for the selected role, an error message appears, and the removal fails.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a role from the right pane and do one of:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When adding a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users or roles currently granted to the role appears. Any user or role with **Administrative only** or **Administrative and role** in the Grant Option column is a role administrator.

4. Select an administrator to be removed.
5. Click **Revoke**.

Note: The **Revoke** button is unavailable if you do not have administrative rights to the selected role.

6. Click **OK**.

See also

- *Adding a Role Administrator to an Existing User-Extended Role* on page 949
- *Modifying a User-Extended Role Administrator's Administrative Rights* on page 951
- *Authenticating a Login Account for a Managed Resource* on page 282

Modifying a User-Extended Role Administrator's Administrative Rights

Modify whether a role administrator can administer a role only or can also use the underlying system privileges and roles of the role being administered.

Prerequisites

Database Version	Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • Administrative rights over the role being managed. • MANAGE ROLES system privilege if the role being granted has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a role from the right pane and do one of:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When adding a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users or roles currently granted to the role appears. Any user or role with **Administrative only** or **Administrative and role** in the Grant Option column is a role administrator.

4. Select an administrator whose administrative rights are to be modified.
5. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

6. Click **OK**.

See also

- *Adding a Role Administrator to an Existing User-Extended Role* on page 949
- *Removing a Role Administrator from a User-Extended Role* on page 950
- *Authenticating a Login Account for a Managed Resource* on page 282

Manage Global Role Administrators of a User-Extended Role

A global role administrator is any user granted the MANAGE ROLES system privilege. However, not all roles can be managed by global role administrators.

When creating a new role, if you specify at least one role administrator, global role administrators will be unable to manage the role. This is because the MANAGE ROLES system privilege is not automatically granted to the role during creation.

For this reason, it is recommended that role administrators not be specified when creating a new role. They should be added after the fact. This ensures that every role can be successfully managed by both role and global role administrators.

By default, at least one role administrator or global role administrator with a login password must exist at all times for each role. This minimum requirement is validated before you can remove the global role administrator or role administrator from a role, or remove a role administrator's administrative rights on a role. The minimum requirement is a configurable database option (**MIN_ROLE_ADMINS**).

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966

DBA User Unable to Manage a User-Extended Role

The **Delete** or **Manage Grantee** menu options are unavailable for a user-extended role.

These menu options are unavailable if the **MANAGE ROLES** system privilege has not been granted to the role as a grantee, and the user has not been designated as a role administrator of the role.

To allow these users to manage the role, either:

- Grant the **MANAGE ROLES** system privilege to the role as a grantee with Administrative only rights, or
- Make the user a role administrator of the role.

The first option is the recommended solution as it allows any user with the **MANAGE ROLES** system privilege to act as a global role administrator of the role, not just the DBA user.

Note: It is strongly recommend that role administrators not be specified when creating a new role. They should be added after the fact. This ensures that all roles can be managed by both role and global role administrators.

See also

- *Adding the Global Role Administrator to a User-Extended Role* on page 954
- *Removing the Global Role Administrator from a User-Extended Role* on page 955

Adding the Global Role Administrator to a User-Extended Role

Add the global role administrator to an existing user-extended role.

Prerequisites

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the role being managed.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

To add the global role administrator, you must add the **MANAGE ROLES** system privilege to the list of grantees (**Manage Grantees**) for the role. Since **MANAGE ROLES** is a system privilege, it may also be added to the list of granted system privileges (**Manage System Privilege**) for the role. However, adding the **MANAGE ROLES** system privilege from the granted system privileges list does not add the global role administrator to the role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantee**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantee**.

Note: The **Manage Grantee** option is unavailable if you do not have rights to manage the role.

4. Click **Grant**.
5. Select **MANAGE ROLES** and click **OK**.

Note: The **MANAGE ROLES** system privilege is not listed if you do not have administrative rights to the privilege.

6. Highlight **MANAGE ROLES**, click in the Grant Option column, and click the arrow. Select **Administrative only**.

Warning! Selecting any other Grant Option results in an error, and the **MANAGE ROLES** system privilege is not granted.

7. Click **OK**.

See also

- *DBA User Unable to Manage a User-Extended Role* on page 954
- *Removing the Global Role Administrator from a User-Extended Role* on page 955
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing the Global Role Administrator from a User-Extended Role

Remove the global role administrator from an existing user-extended role.

Prerequisites

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • Administrative rights over the role being managed. • MANAGE ROLES system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

If revoking membership in a role would result in a failure to meet the minimum number of role administrators for the selected role, an error message appears, and the removal fails.

To remove the global role administrator, you must remove the **MANAGE ROLES** system privilege from the list of grantees (**Manage Grantees**) of the role. Since **MANAGE ROLES** is a system privilege, it may also appear on the list of granted system privileges (**Manage System Privilege**) for the role. Removing the **MANAGE ROLES** system privilege from the granted system privileges list does not remove the global role administrator from the role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantee**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantee**.

Note: The **Manage Grantee** option is unavailable if you do not have rights to manage the role.

4. Select **MANAGE ROLES** and click **Revoke**.

Note:

- The **Revoke** button is unavailable if you do not have administrative rights to the selected system privilege.
-

5. Click **OK**.

See also

- *DBA User Unable to Manage a User-Extended Role* on page 954
- *Adding the Global Role Administrator to a User-Extended Role* on page 954
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating User-Extended Role DDL Commands

Display the SQL data description language for creating a user-extended role. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Role**.
3. Select one or more user-extended roles from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple user-extended roles.

The DDL view opens, showing the SQL code used to create the selected role-based user-extended roles.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966

- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying User-Extended Role Properties

View or change user-extended role properties such as password, login policy and database object permissions.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	<p>View any user-extended role property page – None required.</p> <p>Modify a password – Requires CHANGE PASSWORD system privilege.</p> <p>Modify a login policy, or refresh LDAP DN – Requires MANAGE ANY USER system privilege.</p> <p>Modify a user-extended role comment – Requires one of:</p> <ul style="list-style-type: none">• MANAGE ROLES system privilege.• Administrative rights over the role begin commented. <p>For privileges relating to user-extended role permissions, see:</p> <ul style="list-style-type: none">• <i>Role-Based Database Object Permissions Privilege Summary</i> on page 1034

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a user-extended role from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User-Extended role Properties view appears

4. View or edit the properties.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read only) Name of the user-extended role.</p> <p>Enable Password – Allows the user-extended role to connect to the database with password security. Clearing this option disables the Password and Confirm Password options.</p> <p>Password – The password for the user-extended role. Characters appear as asterisks.</p> <p>Confirm password – A field for confirming the password that you typed in the Password text box. The contents of the two fields must match exactly.</p> <p>Password creation time – Date and time when the password was created.</p> <p>Change password on next login – Select to force the user-extended role to change the password at the next login.</p> <hr/> <p>Note: This functionality is not currently implemented in Sybase Control Center. When logging in to Sybase Control Center, a user will not be prompted to change their password. He or she will be prompted, however, when logging in to SAP Sybase IQ outside of Sybase Control Center (for example, using <i>Interactive SQL</i>).</p> <hr/> <p>Login policy – Select a login policy for the user-extended role from the list.</p> <p>Last login time – Last time the user-extended role successfully logged in.</p> <p>Failed login attempts – Number of times the user-extended role has tried to log in with an incorrect password.</p> <p>Locked – Displays false if the account is unlocked. Displays true if the user-extended role has exceeded the allowed number of failed login attempts.</p> <p>Unlock now –Unlocks the account if Locked is true.</p> <p>Comment – A text field for adding an optional comment about the user-extended role.</p>

Area	Description
Permission	See <i>Role-Based User and Role Object Permissions</i> on page 1008.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing a User-Extended Role Password

Change the password for another role-base user-extended role.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 16.0	Requires CHANGE PASSWORD system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a user-extended role from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User-Extended Role Properties page appears.

4. On the General Properties page, type the new password in the Password and Confirm password fields.
5. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956

- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Forcing a User-Extended Role to Change their Password

Force a role-based user-extended role to change their password the next time he or she logs in.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a user-extended role from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User-Extended Role Properties page appears.

4. On the General Properties page, select **Require password change on next login**.
5. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930

- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Unlocking a User-Extended Role Account

Unlock a locked role-based user-extended role account.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a user-extended role from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The User-Extended Role Properties page appears.

4. On the General Properties page, click **Unlock Now**.
5. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Changing a User-Extended Role Login Policy* on page 965
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing a User-Extended Role Login Policy

Assign a role-based user-extended role a different login policy.

Prerequisites

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > User-Extended Roles**.
3. Select a user-extended role from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The User-Extended Role Properties page appears.

4. On the General Properties page, select a new login policy from the list.
5. Click **OK**.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941

- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Role-Based User-Extended Role Privilege Summary* on page 966
- *Authenticating a Login Account for a Managed Resource* on page 282

Role-Based User-Extended Role Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based user-extended role tasks.

Creating a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Creating a role requires both the MANAGE ANY USER and MANAGE ROLES system privileges.</p> <p>Granting a role during user-extended role creation requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the role being granted (role administrator). • MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>Granting a system privilege during user-extended role creation requires administrative rights over the system privilege being granted.</p>

Deleting a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Converting a User-Extended Role to a Role-Based User

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the role being converted.

Adding and Removing Grantees to and from a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

Changing Administrative Rights of a Grantee of a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

Adding and Removing Underlying Roles to and from a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Changing Administrative Rights on an Underlying Role of a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Adding and Removing System Privileges to and from a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

Changing Administrative Rights on a System Privileges Granted to a User-Extended Role

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

Viewing or Modifying User-Extended Role Options

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	<p>View user-extended role options only – None required.</p> <p>Modify user-extended role options – Depending on the option being modified, requires one of these:</p> <ul style="list-style-type: none"> • SET ANY PUBLIC OPTION system privilege. • SET ANY SECURITY OPTION system privilege. • SET ANY SYSTEM OPTION system privilege.

Managing Role Administrators of a User-Extended Role

Database Version	Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the role being managed. • MANAGE ROLES system privilege if the role being granted has a global role administrator.

Adding the Global Role Administrator to a User-Extended Role

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the role being managed.

Removing the Global Role Administrator from a User-Extended Role

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role being managed. MANAGE ROLES system privilege.

Generating User-Extended Role DDL Commands

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying User-Extended Role Properties

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 16.0	<p>View any user-extended role property page – None required.</p> <p>Modify a password – Requires CHANGE PASSWORD system privilege.</p> <p>Modify a login policy, or refresh LDAP DN – Requires MANAGE ANY USER system privilege.</p> <p>Modify a user-extended role comment – Requires one of:</p> <ul style="list-style-type: none"> MANAGE ROLES system privilege. Administrative rights over the role begin commented. <p>For privileges relating to user-extended role permissions, see:</p> <ul style="list-style-type: none"> <i>Role-Based Database Object Permissions Privilege Summary</i> on page 1034

Changing a User-Extended Role Password

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires CHANGE PASSWORD system privilege.

Forcing a User-Extended Role Password Change

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Unlocking a User-Extended Role Account

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

Changing a User-Extended Role Login Policy

Database Version	Role-Based User-Extended Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege.

See also

- *Creating a User-Extended Role* on page 922
- *Deleting a User-Extended Role* on page 925
- *Converting a User-Extended Role to a User* on page 927
- *Adding a Grantee to a User-Extended Role* on page 928
- *Changing a Grantee's Administrative Rights on a User-Extended Role* on page 930
- *Removing a Grantee From a User-Extended Role* on page 932
- *Adding a Role to a User-Extended Role* on page 933
- *Changing Administrative Rights on an Underlying Role of a User-Extended Role* on page 936
- *Removing a Role from a User-Extended Role* on page 939
- *Adding a System Privilege to a User-Extended Role* on page 941
- *Changing Administrative Rights on a User-Extended Role Granted Privilege* on page 943
- *Removing a System Privilege from a User-Extended Role* on page 944
- *Viewing or Modifying Role-Based User-Extended Role Options* on page 946
- *Manage Role Administrators of a User-Extended Role* on page 947
- *Manage Global Role Administrators of a User-Extended Role* on page 953
- *Generating User-Extended Role DDL Commands* on page 956
- *Viewing or Modifying User-Extended Role Properties* on page 958
- *Changing a User-Extended Role Password* on page 960
- *Forcing a User-Extended Role to Change their Password* on page 962
- *Unlocking a User-Extended Role Account* on page 963
- *Changing a User-Extended Role Login Policy* on page 965

Standalone Roles

Add, change, and delete standalone roles.

Creating a Standalone Role

Add a new standalone role to the database.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Creating a role requires MANAGE ROLES system privilege.</p> <p>Granting a role during standalone role creation requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role being granted (role administrator). MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>Granting a system privilege during standalone creation requires administrative rights over the system privilege being granted.</p>

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Click the arrow next to **Standalone Roles** and select **New**.
The Create Standalone Role Wizard appears.
4. On the Welcome page, specify

Option	Description
Select a resource on which the user will be created.	<p>Select a resource from the list.</p> <hr/> <p>Note: If the selected resource does not support role-based security, an error message appears.</p>
What do you want to name the new user?	Enter a unique user ID.

5. Click **Next**.

6. On the Administrators page, select one or more administrators.

Note: It is strongly recommended that you do not select any role administrators when creating a new role; add them once the creation process is complete. If at least one role administrator is specified during creation, global role administrators will be unable to manage the role because the `MANAGE ROLES` system privilege is not automatically granted to the role.

7. If an administrator is selected, indicate whether the administrator is to be granted membership in the role along with administrative rights (Administrative and role) or administrative rights only (default).

Note: Only one privilege level can be defined for all selected administrators when specified during the create process. However, the privilege level can be later modified. See *Manage Standalone Role Administrators*.

8. Click **Next**.

9. On the Roles page, highlight a role to be granted. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

When you grant a role to a user, user-extended role, or standalone role, unless otherwise noted, any underlying system privileges of the role being granted are automatically inherited by the user, user-extended role, or standalone role.

10. Repeat step 9 to grant additional roles.

11. Click **Next**.

12. On the System Privileges page, highlight a system privilege to be granted. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.

Grant Option	Description
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

13. Repeat step 12 to grant additional privileges.

14. (Optional) On the Comment page, enter a comment for this user.

15. Click **Finish**.

See also

- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Standalone Role

Delete a standalone role from the database.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role being deleted. MANAGE ROLES system privilege if the role being deleted has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security
- The standalone role being deleted does not own any database objects and is not currently connected to the database.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select one or more roles from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple standalone roles.

4. In the Confirm Delete dialog box, click **Revoke role permissions**.
5. Click **Yes** to complete the deletion.

See also

- *Creating a Standalone Role* on page 973
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997

- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282

Adding a Grantee to a Standalone Role

Add a user or role as a member (grantee) of a standalone role. Grantee inherits all underlying system privileges and roles of the standalone role.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • Administrative rights over the role (role administrator). • MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a role from the right pane and either:

- Click the arrow to the right of the name and select **Manage Grantees**, or
- From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When adding a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the role appears.

4. Click **Grant**.
5. Select one or more users or roles to become members.

Tip: Use **Shift-click** or **Control-click** to select multiple users or roles.

6. Click OK.

The new grantees appear with **Role only** rights (no administrative rights)..

7. (Optional) To modify the administrative rights of a role, highlight a role. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

8. Click OK.**See also**

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Changing a Grantee's Administrative Rights on a Standalone Role

Changes a member's (grantee's) ability to manage a standalone role.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Role**.
3. Select a standalone role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When modifying the administrative rights of a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the role appears.

4. Highlight a user or role to be modified. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.

Grant Option	Description
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

5. Click **OK**.

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Removing a Grantee from a Standalone Role

Remove a user or role as a member (grantee) of a standalone role. Grantees lose the ability to use any underlying system privileges or roles of the standalone role.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

By default, a minimum of one role administrator (or global role administrator with a login password) for each role must exist at all times. This minimum requirement is validated before you can remove a member who is a role administrator from a role.

If revoking membership in a role would result in a failure to meet the minimum number of role administrators for the selected role, an error message appears, and the removal fails.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When removing a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the role appears.

4. Highlight a user or role to be removed from the standalone role and click **Revoke**.
5. Click **OK**.

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Adding a Role to a Standalone Role* on page 982

- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Adding a Role to a Standalone Role

Add a role as an underlying role of a standalone role. Members of the standalone role inherit all system privileges and roles of the underlying role, but do not become members of the underlying role. Members of the underlying role do not become members of the standalone role.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the role (role administrator). • MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the underlying role (role administrator). • MANAGE ROLES system privilege if the underlying role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a standalone role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

Warning! When adding an underlying role to a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of underlying roles currently granted to the standalone role appears.

4. Click **Grant**.
5. Select one or more underlying roles to grant.

Tip: Use **Shift-click** or **Control-click** to select multiple roles.

6. Click **OK**.
Newly granted underlying roles appear with **Role only** rights (no administrative rights).
7. (Optional) (For compatibility and user-defined roles only) To modify the administrative rights of an underlying role, highlight a role. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

8. Click **OK**.

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977

- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Changing Administrative Rights on an Underlying Role of a Standalone Role

Changes a member's (grantee's) ability to manage an underlying role of a standalone role.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the role (role administrator). • MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the underlying role (role administrator). • MANAGE ROLES system privilege if the underlying role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

Administrative rights cannot be modified on underlying system roles.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a standalone role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

A list of underlying roles currently granted to the standalone role appears.

4. (Not applicable to system roles) Highlight a role to be modified. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

5. Click **OK**.

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997

- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Removing a Role from a Standalone Role

Remove an underlying role from a standalone role. Grantees of the standalone role lose the ability to use any system privileges of the underlying role or administer the underlying role.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none">• Administrative rights over the role (role administrator).• MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none">• Administrative rights over the underlying role (role administrator).• MANAGE ROLES system privilege if the underlying role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a standalone role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or

- From the Administration Console menu bar, select **Resource > Manage Roles**.

Warning! When removing an underlying role from a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of underlying roles currently granted to the standalone role appears.

4. Highlight a role to be removed and click **Revoke**.
5. Click **OK**.

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Adding a System Privilege to a Standalone Role

Add a system privilege to a standalone role.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a standalone role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the standalone role appears.

4. Click **Grant**.
5. Select one or more system privileges to grant.

Tip: Use **Shift-click** or **Control-click** to select multiple system privilege.

6. Click **OK** to grant the system privilege.
The selected system privileges appear granted with **Privilege only** rights (no administrative rights).
7. (Optional) To modify the administrative rights of a system privilege, highlight a system privilege. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.

Grant Option	Description
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

8. Click **OK**.

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing Administrative Rights on a Privilege Granted to a Standalone Role

Change the administrative rights on a system privilege granted to a standalone role.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a standalone role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the standalone role appears.

4. Highlight a system privilege to be modified. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

5. Click **OK**.

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982

- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing a System Privilege from a Standalone Role

Remove a system privilege from a standalone role.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a standalone role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the standalone role appears.

4. Highlight a system privilege and click **Revoke**.

Note: The **Revoke** button is unavailable if you do not have administrative rights to the selected system privilege.

5. Click **OK**.

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282

Manage Standalone Role Administrators

Role administrators are responsible for granting and revoking standalone roles to users and other roles. You can add and remove role administrators as needed.

There are two types of role administrators:

- Role administrator – users or roles designated to administer a role.
- Global role administrator – any user granted the **MANAGE ROLES** system privilege.

When you create a new role, you can appoint one or more role administrators to manage the role (grant and revoke membership in the role). If no role administrator is specified during the creation process, the **MANAGE ROLES** system privilege is automatically granted to the role with the **Administrative Only** privilege, which creates the global role administrator for a role. However, if at least one administrator is specified during the creation process, the **MANAGE ROLES** system privilege is not granted to the role and global role administrators will be unable to manage the role. For this reason, it is recommended that role administrators not be specified when creating a new role. They should be added after the fact. This ensures that every role can be successfully managed by both role and global role administrators.

A role administrator can add or remove other role administrators from a role, including global role administrators. Both role administrators and global role administrators can grant, revoke,

and drop roles. A role administrator does not require the **MANAGE ROLES** system privilege to administer a role.

By default, at least one role administrator or global role administrator with a login password must exist at all times for each role. This minimum requirement is validated before you can remove the global role administrator or role administrator from a role, or remove a role administrator's administrative rights on a role. The minimum requirement is a configurable database option (**MIN_ROLE_ADMINS**).

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004

Adding a Role Administrator to an Existing Standalone Role

Add a new role administrator to an existing user-extended role.

Prerequisites

Database Version	Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • Administrative rights over the role being managed. • MANAGE ROLES system privilege if the role being granted has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a role from the right pane and do one of:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When adding a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users or roles currently granted to the role appears. Any user or role with **Administrative only** or **Administrative and role** in the Grant Option column is a role administrator.

4. Click **Grant**.
5. Select one or more users or roles. Only roles to which you have administrative rights appear on the list.

Tip: Use **Shift-click** or **Control-click** to select multiple users or roles.

6. Click **OK** to grant membership.
The selected users or roles appear with **Role only** rights (no administrative rights).
7. For each new administrator added, click in the Grant Options column, click the arrow, and select:

Grant Option	Description
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

8. Click **OK**.

See also

- *Removing a Role Administrator from a Standalone Role* on page 995
- *Modifying a Standalone Role Administrator's Administrative Rights* on page 996
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing a Role Administrator from a Standalone Role

Remove a role administrator from an existing user-extended role.

Prerequisites

Database Version	Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role being managed. MANAGE ROLES system privilege if the role being granted has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

By default, at least one role administrator or global role administrator with a login password must exist at all times for each role. This minimum requirement is validated before you can remove the global role administrator or role administrator from a role, or remove a role administrator's administrative rights on a role. The minimum requirement is a configurable database option (**MIN_ROLE_ADMINS**).

If revoking membership in a role would result in a failure to meet the minimum number of role administrators for the selected role, an error message appears, and the removal fails.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a role from the right pane and do one of:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When adding a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users or roles currently granted to the role appears. Any user or role with **Administrative only** or **Administrative and role** in the Grant Option column is a role administrator.

4. Select an administrator to be removed.
5. Click **Revoke**.

Note: The **Revoke** button is unavailable if you do not have administrative rights to the selected role.

6. Click **OK**.

See also

- *Adding a Role Administrator to an Existing Standalone Role* on page 993
- *Modifying a Standalone Role Administrator's Administrative Rights* on page 996
- *Authenticating a Login Account for a Managed Resource* on page 282

Modifying a Standalone Role Administrator's Administrative Rights

Modify whether a role administrator can administer a role only or is also granted the underlying system privileges of the role being administered

Prerequisites

Database Version	Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• Administrative rights over the role being managed.• MANAGE ROLES system privilege if the role being granted has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a role from the right pane and do one of:
 - Click the arrow to the right of the name and select **Manage Grantees**, or

- From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When adding a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users or roles currently granted to the role appears. Any user or role with **Administrative only** or **Administrative and role** in the Grant Option column is a role administrator.

4. Select an administrator whose administrative rights are to be modified.
5. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

6. Click **OK**.

See also

- *Adding a Role Administrator to an Existing Standalone Role* on page 993
- *Removing a Role Administrator from a Standalone Role* on page 995
- *Authenticating a Login Account for a Managed Resource* on page 282

Manage Global Role Administrators of a Standalone Role

A global role administrator is any user granted the MANAGE ROLES system privilege. However, not all roles can be managed by global role administrators.

When creating a new role, if you specify at least one role administrator, global role administrators will be unable to manage the role. This is because the MANAGE ROLES system privilege is not automatically granted to the role during creation.

For this reason, it is recommended that role administrators not be specified when creating a new role. They should be added after the fact. This ensures that every role can be successfully managed by both role and global role administrators.

By default, at least one role administrator or global role administrator with a login password must exist at all times for each role. This minimum requirement is validated before you can remove the global role administrator or role administrator from a role, or remove a role administrator's administrative rights on a role. The minimum requirement is a configurable database option (**MIN_ROLE_ADMINS**).

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004

DBA User or Global Role Administrators Are Unable to Manage a Standalone Role
The **Delete** or **Manage Grantee** menu options are unavailable for a standalone role.

These menu options are unavailable if the **MANAGE ROLES** system privilege has not been granted to the role as a grantee, and the user has not been designated as a role administrator of the role.

To allow these users to manage the role, either:

- Grant the **MANAGE ROLES** system privilege to the role as a grantee with Administrative only rights, or
- Make the user a role administrator of the role.

The first option is the recommended solution as it allows any user with the **MANAGE ROLES** system privilege to act as a global role administrator of the role, not just the DBA user.

Note: It is strongly recommend that role administrators not be specified when creating a new role. They should be added after the fact. This ensures that all roles can be managed by both role and global role administrators.

See also

- *Adding the Global Role Administrator to a Standalone Role* on page 999
- *Removing the Global Role Administrator from a Standalone Role* on page 1000

Adding the Global Role Administrator to a Standalone Role

Add the global role administrator to an existing standalone role.

Prerequisites

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the role being managed.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantee**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantee**.

Note: The **Manage Grantee** option is unavailable if you do not have rights to manage the role.

4. Click **Grant**.
5. Select **MANAGE ROLES** and click **OK**.

Note: The **MANAGE ROLES** system privilege is not listed if you do not have administrative rights to the privilege.

6. Highlight **MANAGE ROLES**, click in the Privileges column, and click the arrow. Select **Administrative only**.

Warning! Selecting any other privilege combination results in an error, and the privilege is not granted.

7. Click **OK**.

See also

- *DBA User or Global Role Administrators Are Unable to Manage a Standalone Role* on page 998
- *Removing the Global Role Administrator from a Standalone Role* on page 1000
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing the Global Role Administrator from a Standalone Role

Remove the global role administrator from an existing standalone role.

Prerequisites

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• Administrative rights over the role being managed.• MANAGE ROLES system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

If revoking membership in a role would result in a failure to meet the minimum number of role administrators for the selected role, an error message appears, and the removal fails.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantee**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantee**.

Note: The **Manage Grantee** option is unavailable if you do not have rights to manage the role.

4. Select **MANAGE ROLES** and click **Revoke**.

Note:

- The **Revoke** button is unavailable if you do not have administrative rights to the selected system privilege.
 - The **MANAGE ROLES** system privilege can also be revoked using the **Manage System Privileges** menu option. However, this revoke does not remove the global role administrator from the role.
-

5. Click **OK**.

See also

- *DBA User or Global Role Administrators Are Unable to Manage a Standalone Role* on page 998
- *Adding the Global Role Administrator to a Standalone Role* on page 999
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Standalone Role DDL Commands

Display the SQL data description language for creating a standalone role. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Role**.
3. Select one or more standalone roles from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple standalone roles.

The DDL view opens, showing the SQL code used to create the selected role-based standalone roles.

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982

- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Role-Based Standalone Role Properties

View or change standalone role comments and database object permissions.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	<p>View any standalone role property page – None required.</p> <p>Modify a standalone role comment – Requires one of:</p> <ul style="list-style-type: none">• Administrative rights over the role being commented.• MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>For privileges relating to standalone role permissions, see:</p> <ul style="list-style-type: none">• <i>Role-Based Database Object Permissions Privilege Summary</i> on page 1034

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.

3. Select a standalone role from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The Standalone Role Properties view appears

4. View or edit the properties.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read only) Name of the standalone role.</p> <p>Comment – A text field for adding an optional comment about the user-extended role.</p>
Permission	See <i>Role-Based User and Role Object Permissions</i> on page 1008.

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Role-Based Standalone Role Privilege Summary* on page 1004
- *Authenticating a Login Account for a Managed Resource* on page 282

Role-Based Standalone Role Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based standalone role tasks.

Creating a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Creating a role requires MANAGE ROLES system privilege.</p> <p>Granting a role during standalone role creation requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role being granted (role administrator). MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>Granting a system privilege during standalone creation requires administrative rights over the system privilege being granted.</p>

Deleting a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role being deleted. MANAGE ROLES system privilege if the role being deleted has a global role administrator.

Adding and Removing Grantees to and from a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

Changing a Grantee's Administrative Rights on a User-Extended Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

Adding and Removing Underlying Roles to and from a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Changing Administrative Rights on an Underlying Role of a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator. <p>To then add an underlying system role requires MANAGE ROLES system privilege.</p> <p>To then add an underlying user-defined or compatibility role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Adding and Removing System Privileges to and from a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

Changing Administrative Rights on a System Privileges Granted to a Standalone Role

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the system privilege. Administrative rights on the role is not required.

Managing Role Administrators of a Standalone Role

Database Version	Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role being managed. MANAGE ROLES system privilege if the role being granted has a global role administrator.

Adding the Global Role Administrator to a Standalone Role

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the role being managed.

Removing the Global Role Administrator from a Standalone Role

Database Version	Global Role Administrator Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role being managed. MANAGE ROLES system privilege.

Generating Standalone Role DDL Commands

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying User-Extended Role Properties

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not Supported.
SAP Sybase IQ 16.0	<p>View any standalone role property page – None required.</p> <p>Modify a standalone role comment – Requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the role being commented. MANAGE ROLES system privilege if the role being granted has a global role administrator. <p>For privileges relating to standalone role permissions, see:</p> <ul style="list-style-type: none"> <i>Role-Based Database Object Permissions Privilege Summary</i> on page 1034

See also

- *Creating a Standalone Role* on page 973
- *Deleting a Standalone Role* on page 975
- *Adding a Grantee to a Standalone Role* on page 977
- *Changing a Grantee's Administrative Rights on a Standalone Role* on page 979
- *Removing a Grantee from a Standalone Role* on page 980
- *Adding a Role to a Standalone Role* on page 982
- *Changing Administrative Rights on an Underlying Role of a Standalone Role* on page 984
- *Removing a Role from a Standalone Role* on page 986
- *Adding a System Privilege to a Standalone Role* on page 988
- *Changing Administrative Rights on a Privilege Granted to a Standalone Role* on page 989
- *Removing a System Privilege from a Standalone Role* on page 991
- *Manage Standalone Role Administrators* on page 992
- *Manage Global Role Administrators of a Standalone Role* on page 997
- *Generating Standalone Role DDL Commands* on page 1001
- *Viewing or Modifying Role-Based Standalone Role Properties* on page 1002

Role-Based Object Permissions on Users and Roles

Permissions on database objects can be granted and revoked to role-based users, user-extended roles, and standalone roles, with or without administrative rights

Role-Based Table or Column Permissions

Permissions on tables and columns can be granted and revoked to role-based users and roles, with or without administrative rights.

About the User or Role Table Permissions List

The Tables permissions list displays permission details the tables and column directly granted to a user, user-extended role, or standalone role

There are several table object permissions, which can be granted with or without administrative rights. Some permissions can be granted at the table level only, while others can be granted at either the table or column level.

- SELECT – table or column level
- INSERT – table level only
- DELETE – table level only
- UPDATE – table or column level
- ALTER – table level only
- REFERENCE – table or column level
- LOAD – table level only
- TRUNCATE – table level only

These object permissions can be granted in several ways:

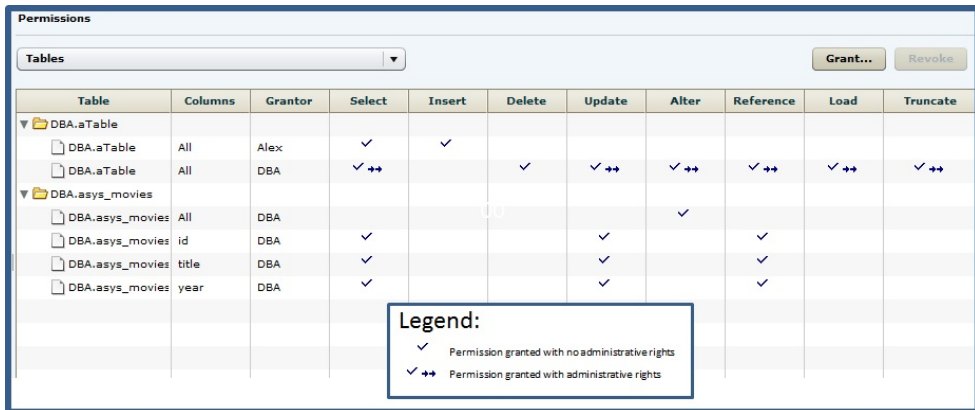
- You own the object.
- You are granted the MANAGE ANY OBJECT PRIVILEGE system privilege.
- You have been indirectly granted specific permissions through membership in a role to which permissions have been directly or indirectly granted.
- You have been directly granted specific permissions.

Users or roles with object ownership or the MANAGE ANY OBJECT PRIVILEGE system privilege are automatically granted all possible object permissions with administrative rights.

Object permissions can be granted with or without administrative rights. When granted without administrative rights, the grantee can perform authorized tasks requiring the permission, but cannot in turn grant the permission to another user or role. When granted with administrative rights (With grant option), the grantee can do both.

The permissions list only lists those tables or columns object permissions granted directly to the selected user or role. The list indicates the table and column the permission is granted on, by who (grantor), and the permissions and their corresponding administrative rights. The permissions list does not list object permissions obtained through ownership, the MANAGE ANY OBJECT PRIVILEGE system privilege, or role membership.

For each table, permissions granted to all columns on the table are listed first (all), followed by each column, sorted alphabetically by column name.



The screenshot shows the 'Permissions' window in SAP Sybase IQ. It features a 'Tables' dropdown menu at the top left, with 'Grant...' and 'Revoke' buttons at the top right. The main table lists permissions for various database objects. A legend box is overlaid on the table, providing a key for the permission symbols.

Table	Columns	Grantor	Select	Insert	Delete	Update	Alter	Reference	Load	Truncate
DBA.aTable										
DBA.aTable	All	Alex	✓	✓						
DBA.aTable	All	DBA	✓ ++		✓	✓ ++	✓ ++	✓ ++	✓ ++	✓ ++
DBA.asys_movies										
DBA.asys_movies	All	DBA					✓			
DBA.asys_movies	id	DBA	✓			✓		✓		
DBA.asys_movies	title	DBA	✓			✓		✓		
DBA.asys_movies	year	DBA	✓			✓		✓		

Legend:
✓ Permission granted with no administrative rights
✓ ++ Permission granted with administrative rights

When granted to a role, permissions, including administrative rights, are inherited by all members of the role. The role, not the users indirectly granted the permissions through inheritance, appear on the permissions list.

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the SELECT permission with the With grant option. UserA grants SELECT to UserB with the With grant option. UserB grants SELECT to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the SELECT permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

Permissions can be granted on the same table or column, by multiple grantors, resulting in the same table or column appearing multiple times on the list. If the same permission is granted to the same table or column, with and without administrative rights, the grant with the administrative right takes precedence.

The screenshot shows the 'Permissions' window in SAP Sybase IQ. It displays a table named 'DBA.aTable' with columns 'Table', 'Columns', 'Grantor', 'Select', 'Insert', 'Delete', 'Update', 'Alter', 'Reference', 'Load', and 'Truncate'. The table has two rows: one for 'DBA.aTable' with 'All' columns, granted to 'Alex' with 'Select' and 'Insert' permissions, and another for 'DBA.aTable' with 'All' columns, granted to 'DBA' with 'Select', 'Delete', 'Update', 'Alter', 'Reference', 'Load', and 'Truncate' permissions. The permissions for Alex and DBA are highlighted with a red box.

Table	Columns	Grantor	Select	Insert	Delete	Update	Alter	Reference	Load	Truncate
DBA.aTable	All	Alex	✓	✓						
DBA.aTable	All	DBA	✓ ++		✓	✓ ++	✓ ++	✓ ++	✓ ++	✓ ++

In this example, the user is granted the SELECT permission by both DBA and Alex, with different administrative rights. When the same permission is granted with different administrative rights, the higher administrative right takes precedence.

When revoking a permission granted multiple times, the permission is revoked from all instances, regardless of administrative rights. For example, Manager1 grants User2 INSERT with administrative rights. User1 also grants INSERT to User2, but without administrative rights. Regardless of which instance of INSERT is revoked, both instances of INSERT are revoked for User2.

Following the User or Role Table Permissions Grant Trail

Before revoking a grantee's permission, you need to identify grantees directly or indirectly granted the permission from the original grantee.

The grant chain traces how a grantee has in turn granted a permission to other grantees.

However, when you view the object permissions granted to a specific user, user-extended role, or standalone role, you only see the permissions granted to the selected user or role. You do not see who the user or role has granted the permissions to.

To determine who the selected user or role has in turn granted an object permission to, note the table, column name (if applicable), and the permission to be traced, then display the permissions list for the table object to be traced. See *Setting Table Permissions > Following the Table Permissions Grant Trail* for details.

Removing Permissions on a Table or Column from a User or Role

Remove permissions on a table or column from a user, user-extended role, or standalone role.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You have administrative rights (with grant option) to the permission. You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the SELECT permission with the `With grant option`. UserA grants SELECT to UserB with the `With grant option`. UserB grants SELECT to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the SELECT permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
4. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. In the right pane, expand the table containing the permission to be revoked.
7. Highlight the row containing the permission to be modified.

Note: If the permission appears on the list multiple times with different grantors, with or without administrative rights, it does not matter which instance is selected.

8. Click **Revoke**.

A list of permissions currently granted (regardless of administrative rights) appears.

9. Select one or more permissions to revoke. Click the box in the header row to select all available permissions.

Warning! Revoking permissions may result in unexpected revocation from other users or groups. See *Following the User or Role Table Permission Grant Trail*.

10. Click **Finish**.

11. Click **OK**.

Note: The expanded table structure collapses, appearing as if all permissions were revoked, instead of the selected permission. Re-expand the table to view the remaining permissions.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Adding Permissions on a Table or Column to a User or Role

Add permissions on a table or column to a user, user-extended role, or standalone role.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**

- **User-Extended Roles**
 - **Standalone Roles**
4. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
 5. In the left pane, select **Permissions**.
 6. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
 7. On the Welcome page, based on the table level to which permission is being granted, select **Tables** or **Table columns**.
 8. Click **Next**.
 9. Do one of:

Choice	Action
If Tables was selected	Select the table to apply permissions to. Click the box in the header row to select all available tables.
If Table Column was selected	<ul style="list-style-type: none"> • Click the Table drop-down arrow and select the table containing the column to which permissions are to be applied. • Select one or more columns to apply permissions to. Click the box in the header row to select all available columns on the table.

10. Click **Next**.
11. On the Permissions page, select one or more permissions. Click the box in the header row to select all available permissions.
12. (Optional) Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

13. Click **Finish**.
14. Click **OK**.

Note: To view the permissions granted on a table or column, click to expand the table name in the Table column.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Adding Administrative Rights on a Granted Table or Column Permission to a User or Role

Add user or role administrative rights only to a granted table or column permission.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You have administrative rights to the permission being modified. You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
4. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
7. On the Welcome page, based on the table level of the existing permission to be granted administrative rights, select **Tables** or **Table columns**.
8. Click **Next**.
9. Do one of:

Choice	Action
If Tables was selected	Select the table containing the existing permission to which apply administrative rights are to be applied.
If Table Column was selected	<ul style="list-style-type: none"> Click the Table drop-down arrow and select the table containing the column to which administrative rights are to be applied. Select the columns containing the existing permission to which apply administrative rights are to be applied.

10. Click **Next**.

11. On the Permissions page, select the granted permissions to which administrative rights are to be granted.

12. Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

13. Click **Finish**.

14. Click **OK**.

Note: To view the permissions granted on a table or column, click to expand the table name in the Table column.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Removing Administrative Rights Only on a Table or Column Permission from a User or Role

Remove administrative rights only from a permission granted to a user, user-extended role, or standalone role, on a table or column.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You have administrative rights to the permission being modified. You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports role-based security
- You are logged on as the original grantor of the permission with administrative rights to be removed.

Task

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
4. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. In the right pane, click **Grant**.
7. On the Welcome page, based on the table level of the permission to be regranted, select **Tables** or **Table columns**.
8. Click **Next**.

9. On the Permissions page, select the permissions from which the administrative rights are being revoked.

10. Click **Finish**.

11. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Role-Based View or Materialized View Permissions

Grant permissions on a view or materialized view to a user, user-extended role, or standalone role.

About the User or Role View Permissions List

The Views permissions list displays permission details the tables and column directly granted to a user, user-extended role, or standalone role.

There are four object permissions for views or materialized views, which can be granted with or without administrative rights:

- SELECT
- INSERT
- DELETE
- UPDATE

These object permissions can be granted in several ways:

- You own the object.
- You are granted the MANAGE ANY OBJECT PRIVILEGE system privilege.
- You have been indirectly granted specific permissions through membership in a role to which permissions have been directly or indirectly granted.
- You have been directly granted specific permissions.

Users or roles with object ownership or the MANAGE ANY OBJECT PRIVILEGE system privilege are automatically granted all possible object permissions with administrative rights.

Object permissions can be granted with or without administrative rights. When granted without administrative rights, the grantee can perform authorized tasks requiring the permission, but cannot in turn grant the permission to another user or role. When granted with administrative rights (With grant option), the grantee can do both.

The permissions list only lists those view and materialized view object permissions granted directly to the selected user or role. The list indicates the view or materialized view the permission is granted on, by who (grantor), and the permissions and their corresponding administrative rights. The permissions list does not list object permissions obtained through ownership, the MANAGE ANY SYSTEM OBJECT system privilege, or role membership.

The permissions list is sorted alphabetically by Grantor.

View	Grantor	Select	Insert	Delete	Update
DBA.cView	Alex	✓	✓ ↔	✓ ↔	
DBA.bView	DBA	✓ ↔		✓	✓ ↔

Legend:

- ✓ Permission granted with no administrative rights
- ✓ ↔ Permission granted with administrative rights

When granted to a role, permissions, including administrative rights, are inherited by all members of the role. The role, not the users indirectly granted the permissions through inheritance, appear on the permissions list.

The REVOKE command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the SELECT permission with the With grant option. UserA grants SELECT to UserB with the With grant option. UserB grants SELECT to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the SELECT permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

Permissions can be granted on the same view or materialized view, by multiple grantors, resulting in the same view or materialized view appearing multiple times on the list. If the same permission is granted to the same view or materialized view, with and without administrative rights, the grant with the administrative right takes precedence.

View	Grantor	Select	Insert	Delete	Update
DBA.cView	Alex	✓	✓ ↔	✓ ↔	
DBA.bView	DBA	✓ ↔		✓	✓ ↔
DBA.cView	DBA	✓ ↔	✓		

When revoking a permission granted multiple times, the permission is revoked from all instances, regardless of administrative rights. For example, Manager1 grants User2 INSERT with administrative rights. User1 also grants INSERT to User2, but without administrative rights. Regardless of which instance of INSERT is revoked, both instances of INSERT are revoked for User2.

Following the User or Role View Permission List

Before revoking a grantee's permission, you need to identify grantees directly or indirectly granted the permission from the original grantee.

The grant chain traces how a grantee has in turn granted a permission to other grantees.

However, when you view the object permissions granted to a specific user, user-extended role, or standalone role, you only see the permissions granted to the selected user or role. You do not see who the user or role has granted the permissions to.

To determine who the selected user or role has in turn granted an object permission to, note the table, column name (if applicable), and the permission to be traced, then display the permissions list for the table object to be traced. See *Setting View Permissions > Following the View Permissions Grant Trail* or *Setting Materialized View Permissions > Following the Materialized View Permissions Grant Trail* for details.

Adding View or Materialized View Permissions to a User or Role

Add permissions on a view or materialized view to a user, user-extended role, or standalone role.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You have administrative rights (with grant option) to the permission. You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
4. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. Click the drop-down arrow and select **Views**.
A list of permissions currently granted to **Views** appears.
7. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
8. Select **Views**.
9. Click **Next**.
10. On the Objects page, select the view or materialized view on which the permission is being granted.
11. Click **Next**.
12. On the Permissions page, select one or more permissions. Click the box in the header row to select all available permissions.
13. (Optional) Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

14. Click **Finish**.

15. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Removing View or Materialized View Permissions from a User or Role

Remove permissions from a view or materialized view to a user, user-extended role, or standalone role.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports role-based security

Task

The **REVOKE** command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

If multiple permissions are granted, you can revoke some or all of the permissions. However, if you revoke a permission granted administrative rights, and the grantee has granted the

permission to other users, who in turn have granted it to other users, and so on, every grantee in the chain who has received the permission indirectly, with or without administrative rights, also has their permission revoked. For example, UserA is granted the **SELECT** permission with the **With grant option**. UserA grants **SELECT** to UserB with the **With grant option**. UserB grants **SELECT** to UserC and UserD without administrative rights and to UserE with administrative rights. When you revoke the **SELECT** permission from UserA, it is also revoked for UserB, UserC, UserD and UserE.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
4. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. Click the drop-down arrow and select **Views**.
A list of permissions currently granted to **Views** appears.
7. In the right pane, select the view or materialized view containing the permission to be revoked and click **Revoke**.
A list of permissions currently granted (regardless of administrative rights) appears.
8. Select one or more permissions to revoke. Click the box in the header row to select all available permissions.

Warning! Revoking permissions may result in unexpected revocation from other users or groups. See *Following the User or Role View Permission Grant Trail*.

9. Click **Finish**.
10. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Removing Administrative Rights Only on a View or Materialized Permission from a User or Role

Remove administrative rights only from a permission granted to a user, user-extended role, or standalone role on a view or materialized view.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You have administrative rights to the permission being modified.• You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports role-based security
- You are logged on as the original grantor of the permission with administrative rights to be removed.

Task

The **REVOKE** command applies to the database object permission itself, not to any administrative right granted on the permission. Therefore, to remove the administrative right only and leave the database object permission intact, do not use the **Revoke** button. Rather, regrant the specific permission without administrative rights. Only the original grantor can remove the administrative rights only from a granted permission. If another grantor regrants the same permission without administrative rights, a new permission without administrative rights is granted, but the original permission with administrative rights remains and takes precedence over any other non-administrative grants of the same permission to the same user or role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**

4. Select:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

5. In the left pane, select Permissions.**6. Click the drop-down arrow and select Views.**

A list of permissions currently granted to **Views** appears.

7. In the right pane, click Grant.**8. Select Views.****9. Click Next.****10. On the Objects page, select the view or materialized view on which the administrative rights on a permissible are being removed.****11. Click Next.****12. On the Permissions page, select the permissions from which the administrative rights are being revoked.****13. Click Finish.****14. Click OK.****See also**

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Adding Administrative Rights to a Granted View Permission to a User or Role

Add administrative rights only to a granted view or materialized view permission.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
4. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. Click the drop-down arrow and select **Views**.
A list of permissions currently granted to **Views** appears.
7. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
8. Select **Views**.
9. Click **Next**.
10. On the Objects page, select the view or materialized view on which the existing permission to be granted administrative rights resides.
11. Click **Next**.
12. On the Permissions page, select the permission to which administrative rights are to be granted.
13. Click the **With grant option** to grant the selected permissions administrative rights.

Note: The **With grant option** applies to all selected permissions. You cannot apply the **With grant option** option to individual permissions.

14. Click **Finish**.
15. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Role-Based Procedure or Function Permission

Grant and revoke execute permission on a function, procedure, dbspace, or sequence generator for a user, user-extended role, or standalone role.

Adding EXECUTE Permission to a User or Role

Add execute permission on a function or procedure to a user, user-extended role, or standalone role.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. Navigate to the applicable **Users**, **User-Extended Roles**, or **Standalone Roles** properties page.
2. In the left pane, click **Permissions**.
3. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
4. In the left pane, select **IQ Servers > Security > Role-Based**.
5. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
6. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
7. In the left pane, select **Permissions**.
8. Click the drop-down arrow and select **Procedures** or **Functions**.
A list of permissions currently granted to **Procedures** or **Functions** appears.
9. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
10. On the Welcome page, select **Procedures** or **Functions**.

11. Click **Next**.
12. On the Objects page, select one or more objects to grant execute permission to.

Tip: Use **Shift-click** or **Control-click** to select multiple objects.

13. Click **Next**.
14. On the Permissions page, select **Execute**.
15. Click **Finish**.
16. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Removing EXECUTE Permission from a User or Role

Remove execute permission on a function or procedure to a user, user-extended role, or standalone role.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
4. Select:

- Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
 6. Click the drop-down arrow and select **Procedures** or **Functions**.
A list of permissions currently granted to **Procedures** or **Functions** appears.
 7. In the right pane, highlight the permission to be revoked and click **Revoke**.
 8. At the confirmation prompt, click **Yes**.
 9. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Role-Based Dbspace Permission

Grant and revoke create permission on a dbspace for a user, user-extended role, or standalone role.

Adding CREATE Permission to a User or Role

Add create permission on a dbspace to a user, user-extended role, or standalone role.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**

4. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. Click the drop-down arrow and select **Dbspaces**.
A list of permissions currently granted to **Dbspaces** appears.
7. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
8. On the Welcome page, select **Dbspaces**.
9. Click **Next**.
10. On the Objects page, select one or more objects to grant create permission to.

Tip: Use **Shift-click** or **Control-click** to select multiple objects.

11. Click **Next**.
12. On the Permissions page, select **Create**.
13. Click **Finish**.
14. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Removing CREATE Permission to User or Role

Remove create permission on a dbspace to a user, user-extended role, or standalone role.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
4. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. Click the drop-down arrow and select **Dbspaces**.
A list of permissions currently granted to **Dbspaces** appears.
7. In the right pane, highlight the permission to be revoked and click **Revoke**.
8. At the confirmation prompt, click **Yes**.
9. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Role-Based Sequence Generator Permission

Grant and revoke usage permission on a sequence generator for a user, user-extended role, or standalone role.

Adding USAGE Permission to a User or Role

Add usage permission on a sequence generator to a user, user-extended role, or standalone role.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the sequence generator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. Navigate to the applicable **Users**, **User-Extended Roles**, or **Standalone Roles** properties page.
2. In the left pane, click **Permissions**.
3. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
4. In the left pane, select **IQ Servers > Security > Role-Based**.
5. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
6. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
7. In the left pane, select **Permissions**.
8. Click the drop-down arrow and select **Sequence Generators**.
A list of permissions currently granted to **Sequence Generators** appears.
9. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
10. On the Welcome page, select **Sequence Generators**.
11. Click **Next**.
12. On the Objects page, select one or more objects to grant usage permission to.

Tip: Use **Shift-click** or **Control-click** to select multiple objects.

13. Click **Next**.
14. On the Permissions page, select **Usage**.
15. Click **Finish**.
16. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Removing USAGE Permission from a User or Role

Remove usage permission on a sequence generator from a user, user-extended role, or standalone role.

Prerequisites

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You own the sequence generator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based**.
3. Select:
 - **Users**
 - **User-Extended Roles**
 - **Standalone Roles**
4. Select:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
5. In the left pane, select **Permissions**.
6. Click the drop-down arrow and select **Sequence Generators**.
A list of permissions currently granted to **Sequence Generators** appears.
7. In the right pane, highlight the permission to be revoked and click **Revoke**.
8. At the confirmation prompt, click **Yes**.
9. Click **OK**.

See also

- *Authenticating a Login Account for a Managed Resource* on page 282
- *Role-Based Database Object Permissions Privilege Summary* on page 1034

Role-Based Database Object Permissions Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based user, user-extended role, or standalone role tasks relating to database objects.

Grant or Revoke Permissions on a Table or Column

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

Modify Administrative Permissions on a Table or Column

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights to the permission being modified. • You own the database object.

Grant or Revoke Permissions on a View or Materialized View

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You have administrative rights (with grant option) to the permission. • You own the database object.

Modify Administrative Permissions on a View or Materialized View

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You have administrative rights to the permission being modified. You own the database object.

Grant or Revoke Permissions on a Function or Procedure

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You own the database object.

Grant or Revoke Permissions on a Sequence Generator

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You own the sequence generator.

Grant or Revoke Permissions on a Dbspace

Database Version	Role-Based Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

System Roles

System roles are automatically created in each newly created or database and has been granted specific system privileges.

You can grant and revoke system roles to users and roles, but you cannot delete them. System roles cannot own objects.

System Role Name	Authorized Tasks Supported
diagnostics	Allows users to run diagnostic operations. The diagnostics system role owns the diagnostic tables and views.
rs_systabgroup	Allows users to perform replication server functionality.
SA_DEBUG	Allows users to use the SQL Anywhere Debugger.
SYS_REPLICATION_ADMIN_ROLE	Allows users to perform replication related administration tasks.
SYS_RUN_REPLICATION_ROLE	Allows users to perform replication tasks using the dbremote utility and synchronization tasks using the dbmlsync utility.
SYS_SPATIAL_ADMIN_ROLE	Allows users to create, alter, drop, or comment on spatial reference systems and spatial units of measure. The SYS_SPATIAL_ADMIN_ROLE is the owner of all spatial objects.
SYS	The SYS role owns the system tables and views for the database, which contain the full description of database schema, including all database objects and all user IDs. The SYS system role can be granted to other roles with no administrative rights only.
dbo	The dbo system role owns many system stored procedures and views.
PUBLIC	The PUBLIC system role has SELECT permission on the system tables.

View Grantees of a System Role

Display a list of the users and roles granted membership to a system role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > System Roles**.
3. Select a system role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When viewing a list of grantees to a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of grantees granted to the system role along with their corresponding grant option appears.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

See also

- *View Underlying Roles of a System Role* on page 1038
- *View System Privileges Granted to a System Role* on page 1039

- *Adding a Grantee to a System Role* on page 1041
- *Removing a Grantee from a System Role* on page 1042
- *Adding a Role to a System Role* on page 1043
- *Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- *Removing a Role from a System Role* on page 1048
- *Adding a System Privilege to a System Role* on page 1049
- *Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- *Removing a System Privilege from a System Role* on page 1052
- *Role-Based System Role Privilege Summary* on page 1053
- *Authenticating a Login Account for a Managed Resource* on page 282

View Underlying Roles of a System Role

Display a list of the underlying roles granted to a system role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

You cannot modify or remove the underlying roles granted to a system role, but you can add and remove additional underlying roles to the role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > System Roles**.
3. Select a system role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

Warning! When viewing a list of the underlying role of a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of underlying roles granted to the system role along with their corresponding grant option appears.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

See also

- *View Grantees of a System Role* on page 1037
- *View System Privileges Granted to a System Role* on page 1039
- *Adding a Grantee to a System Role* on page 1041
- *Removing a Grantee from a System Role* on page 1042
- *Adding a Role to a System Role* on page 1043
- *Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- *Removing a Role from a System Role* on page 1048
- *Adding a System Privilege to a System Role* on page 1049
- *Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- *Removing a System Privilege from a System Role* on page 1052
- *Role-Based System Role Privilege Summary* on page 1053
- *Authenticating a Login Account for a Managed Resource* on page 282

View System Privileges Granted to a System Role

Display a list of the system privileges granted to a system role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > System Roles**.
3. Select a system role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges granted to the system role along with their corresponding grant option appears.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

See also

- *View Grantees of a System Role* on page 1037
- *View Underlying Roles of a System Role* on page 1038
- *Adding a Grantee to a System Role* on page 1041
- *Removing a Grantee from a System Role* on page 1042
- *Adding a Role to a System Role* on page 1043
- *Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- *Removing a Role from a System Role* on page 1048
- *Adding a System Privilege to a System Role* on page 1049
- *Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- *Removing a System Privilege from a System Role* on page 1052
- *Role-Based System Role Privilege Summary* on page 1053
- *Authenticating a Login Account for a Managed Resource* on page 282

Adding a Grantee to a System Role

Add a user or role as a member (grantee) of a system role. Grantee inherits all underlying system privileges and roles of the system role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

Grantees cannot be granted administrative rights on a system role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > System Roles**.
3. Select a system role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When adding a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the system role appears.

4. Click **Grant**.
5. Select one or more user or roles to grant.

Tip: Use **Shift-click** or **Control-click** to select multiple users or roles.

6. Click **OK**.
The selected grantees appear with **Role only** rights (no administrative rights).
7. Click **OK**.

See also

- *View Grantees of a System Role* on page 1037
- *View Underlying Roles of a System Role* on page 1038

- *View System Privileges Granted to a System Role* on page 1039
- *Removing a Grantee from a System Role* on page 1042
- *Adding a Role to a System Role* on page 1043
- *Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- *Removing a Role from a System Role* on page 1048
- *Adding a System Privilege to a System Role* on page 1049
- *Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- *Removing a System Privilege from a System Role* on page 1052
- *Role-Based System Role Privilege Summary* on page 1053
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Removing a Grantee from a System Role

Remove a user or role as a member of a system role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > System Roles**.
3. Select a system role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When removing a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the system role appears.

4. Highlight a user or role to be removed and click **Revoke**.
5. Click **OK**.

See also

- *View Grantees of a System Role* on page 1037
- *View Underlying Roles of a System Role* on page 1038
- *View System Privileges Granted to a System Role* on page 1039
- *Adding a Grantee to a System Role* on page 1041
- *Adding a Role to a System Role* on page 1043
- *Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- *Removing a Role from a System Role* on page 1048
- *Adding a System Privilege to a System Role* on page 1049
- *Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- *Removing a System Privilege from a System Role* on page 1052
- *Role-Based System Role Privilege Summary* on page 1053
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Adding a Role to a System Role

Add a role as an underlying role of a standalone role. Members of the system role inherit the system privileges of the underlying role, but do not become members of the underlying role. Members of the underlying role do not become members of the standalone role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires the MANAGE ROLES system privilege.</p> <p>To then add an underlying role requires one of:</p> <ul style="list-style-type: none"> • Administrative rights over the underlying role (role administrator). • MANAGE ROLES system privilege if the underlying role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.

- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > System Roles**.
3. Select a system role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

Warning! When adding an underlying role to a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of underlying roles currently granted to the system role appears.

4. Click **Grant**.
5. Select one or more underlying roles to grant.

Tip: Use **Shift-click** or **Control-click** to select multiple roles.

6. Click **OK** to grant the role.
Newly granted underlying roles appear with **Role only** rights (no administrative rights).
7. (Optional) (For compatibility and user-defined roles only) To modify the administrative rights of an underlying role, highlight a role. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

Note: The following steps represent a behavior change with SAP Sybase IQ 16.0, for the following roles only.

- SYS_AUTH_DBA_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_RUN_REPLICATION_ROLE
- SYS_AUTH_RESOURCE_ROLE

- **SYS_AUTH_VALIDATE_ROLE**

Prior to 16.0, when granting membership to one of these roles, the default inheritance behavior was to not allow members of the role to automatically inherit the underlying system privileges and roles of the compatibility role. Only the log on user (of the role) would inherit. As of 16.0, the default behavior is to allow automatic inheritance by all members of the role.

8. (Optional for SYS_AUTH_DBA_ROLE only) To prevent automatic inheritance of the SYS_AUTH_DBA_ROLE when granted with the **Administrative and Role** option, click in the Inheritance column, and select No Inheritance.
9. (Optional for SYS_AUTH_DBA_ROLE, SYS_AUTH_BACKUP_ROLE, SYS_RUN_REPLICATION_ROLE, SYS_AUTH_RESOURCE_ROLE, or SYS_AUTH_VALIDATE_ROLE only) To prevent automatic inheritance when granted with **Role only** option, click in the Inheritance column, and select No Inheritance.
10. Click **OK**.

See also

- *View Grantees of a System Role* on page 1037
- *View Underlying Roles of a System Role* on page 1038
- *View System Privileges Granted to a System Role* on page 1039
- *Adding a Grantee to a System Role* on page 1041
- *Removing a Grantee from a System Role* on page 1042
- *Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- *Removing a Role from a System Role* on page 1048
- *Adding a System Privilege to a System Role* on page 1049
- *Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- *Removing a System Privilege from a System Role* on page 1052
- *Role-Based System Role Privilege Summary* on page 1053
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Changing Administrative Rights on an Underlying Role of a System Role

Changes a member's (grantee's) ability to manage an underlying role of a system role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires the MANAGE ROLES system privilege.</p> <p>To then add an underlying role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

Administrative rights on any default underlying roles of a system role cannot be changed.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Standalone Roles**.
3. Select a standalone role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

Warning! When modifying the administrative rights of a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of underlying roles currently granted to the standalone role appears.

4. (Not applicable to system roles) Highlight a role to be modified. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

Note: The following steps represent a behavior change with SAP Sybase IQ 16.0, for the following roles only.

- SYS_AUTH_DBA_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_RUN_REPLICATION_ROLE
- SYS_AUTH_RESOURCE_ROLE
- SYS_AUTH_VALIDATE_ROLE

Prior to 16.0, when granting membership to one of these roles, the default inheritance behavior was to not allow members of the role to automatically inherit the underlying system privileges and roles of the compatibility role. Only the log on user (of the role) would inherit. As of 16.0, the default behavior is to allow automatic inheritance by all members of the role.

5. (Optional for SYS_AUTH_DBA_ROLE only) To prevent automatic inheritance of the SYS_AUTH_DBA_ROLE when granted with the **Administrative and Role** option, click in the Inheritance column, and select No Inheritance.
6. (Optional for SYS_AUTH_DBA_ROLE, SYS_AUTH_BACKUP_ROLE, SYS_RUN_REPLICATION_ROLE, SYS_AUTH_RESOURCE_ROLE, or SYS_AUTH_VALIDATE_ROLE only) To prevent automatic inheritance when granted with **Role only** option, click in the Inheritance column, and select No Inheritance.
7. Click **OK**.

See also

- *View Grantees of a System Role* on page 1037
- *View Underlying Roles of a System Role* on page 1038
- *View System Privileges Granted to a System Role* on page 1039
- *Adding a Grantee to a System Role* on page 1041
- *Removing a Grantee from a System Role* on page 1042
- *Adding a Role to a System Role* on page 1043
- *Removing a Role from a System Role* on page 1048
- *Adding a System Privilege to a System Role* on page 1049
- *Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- *Removing a System Privilege from a System Role* on page 1052
- *Role-Based System Role Privilege Summary* on page 1053
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Removing a Role from a System Role

Remove a role as an underlying role of a system role. Members of the system role lose the ability to use any system privileges of the underlying role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires the MANAGE ROLES system privilege.</p> <p>To then add an underlying role requires one of:</p> <ul style="list-style-type: none">• Administrative rights over the underlying role (role administrator).• MANAGE ROLES system privilege if the underlying role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

Default underlying roles of a system role cannot be revoked.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > System Roles**.
3. Select a system role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

Warning! When removing an underlying role from a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of underlying roles currently granted to the system role appears.

4. Highlight a role to be removed and click **Revoke**.

Note: The **Revoke** button is unavailable if the selected role is a default underlying role of the system role, or you do not have administrative rights to the role.

5. Click **OK**.

See also

- *View Grantees of a System Role* on page 1037
- *View Underlying Roles of a System Role* on page 1038
- *View System Privileges Granted to a System Role* on page 1039
- *Adding a Grantee to a System Role* on page 1041
- *Removing a Grantee from a System Role* on page 1042
- *Adding a Role to a System Role* on page 1043
- *Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- *Adding a System Privilege to a System Role* on page 1049
- *Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- *Removing a System Privilege from a System Role* on page 1052
- *Role-Based System Role Privilege Summary* on page 1053
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Adding a System Privilege to a System Role

Add a system privilege to a system role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege along with administrative rights over the system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > System Roles**.
3. Select a system role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or

- From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the system role appears.

- Click **Grant**.
- Select one or more system privileges to grant.

Tip: Use **Shift-click** or **Control-click** to select multiple system privilege.

- Click **OK** to grant the system privilege.
The selected system privileges appear granted with **Privilege only** rights (no administrative rights).
- (Optional) To modify the administrative rights of a system privilege, highlight a system privilege. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

- Click **OK**.

See also

- View Grantees of a System Role* on page 1037
- View Underlying Roles of a System Role* on page 1038
- View System Privileges Granted to a System Role* on page 1039
- Adding a Grantee to a System Role* on page 1041
- Removing a Grantee from a System Role* on page 1042
- Adding a Role to a System Role* on page 1043
- Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- Removing a Role from a System Role* on page 1048
- Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- Removing a System Privilege from a System Role* on page 1052
- Role-Based System Role Privilege Summary* on page 1053
- Authenticating a Login Account for a Managed Resource* on page 282

Changing Administrative Rights on a System Role Granted Privilege

Change the administrative rights on a system privilege granted to a system role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege along with administrative rights over the system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

You cannot change the administrative rights on the default underlying system privileges of a system role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > System Roles**.
3. Select a system role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the system role appears.

4. Highlight a system privilege to be modified. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.

Grant Option	Description
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

5. Click **OK**.

See also

- *View Grantees of a System Role* on page 1037
- *View Underlying Roles of a System Role* on page 1038
- *View System Privileges Granted to a System Role* on page 1039
- *Adding a Grantee to a System Role* on page 1041
- *Removing a Grantee from a System Role* on page 1042
- *Adding a Role to a System Role* on page 1043
- *Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- *Removing a Role from a System Role* on page 1048
- *Adding a System Privilege to a System Role* on page 1049
- *Removing a System Privilege from a System Role* on page 1052
- *Role-Based System Role Privilege Summary* on page 1053
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing a System Privilege from a System Role

Remove a system privilege from a system role.

Prerequisites

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege along with administrative rights over the system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

You cannot remove the underlying system privilege granted to a system role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Security > Role-Based > System Roles**.
3. Select a system role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges currently granted to the system role appears.

4. Highlight a system privilege and click **Revoke**.

Note: The **Revoke** button is unavailable if the selected system privilege is a default underlying system privilege of the system role, or you do not have administrative rights to the system privilege.

5. Click **OK**.

See also

- *View Grantees of a System Role* on page 1037
- *View Underlying Roles of a System Role* on page 1038
- *View System Privileges Granted to a System Role* on page 1039
- *Adding a Grantee to a System Role* on page 1041
- *Removing a Grantee from a System Role* on page 1042
- *Adding a Role to a System Role* on page 1043
- *Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- *Removing a Role from a System Role* on page 1048
- *Adding a System Privilege to a System Role* on page 1049
- *Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- *Role-Based System Role Privilege Summary* on page 1053
- *Authenticating a Login Account for a Managed Resource* on page 282

Role-Based System Role Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based system role tasks.

View Grantees, Underlying Roles, and System Privileges Granted to a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Adding and Removing Grantees to and from a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege.

Adding and Removing Underlying Roles to and from a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires the MANAGE ROLES system privilege.</p> <p>To then add an underlying role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Changing Administrative Rights of an Underlying Role on a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	<p>To enable the Manage Roles option requires the MANAGE ROLES system privilege.</p> <p>To then add an underlying role requires one of:</p> <ul style="list-style-type: none"> Administrative rights over the underlying role (role administrator). MANAGE ROLES system privilege if the underlying role has a global role administrator.

Adding and Removing System Privileges from a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege along with administrative rights over the system privilege.

Changing Administrative Rights of an Underlying Role on a System Role

Database Version	Role-Based System Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ROLES system privilege along with administrative rights over the system privilege.

See also

- *View Grantees of a System Role* on page 1037
- *View Underlying Roles of a System Role* on page 1038
- *View System Privileges Granted to a System Role* on page 1039
- *Adding a Grantee to a System Role* on page 1041
- *Removing a Grantee from a System Role* on page 1042
- *Adding a Role to a System Role* on page 1043
- *Changing Administrative Rights on an Underlying Role of a System Role* on page 1045
- *Removing a Role from a System Role* on page 1048
- *Adding a System Privilege to a System Role* on page 1049
- *Changing Administrative Rights on a System Role Granted Privilege* on page 1051
- *Removing a System Privilege from a System Role* on page 1052

Compatibility Roles

Compatibility roles are automatically created in each newly created or database and has been granted specific system privileges.

You can grant and revoke compatibility roles to users and roles. They can be migrated to standalone roles and dropped under specific conditions. Compatibility role names begin with SYS_AUTH_ and end with _ROLE. Also called predefined roles, they are created for backward compatibility with earlier versions of SAP Sybase IQ.

Compatibility Role Name	Authorized Tasks Supported
SYS_AUTH_SA_ROLE	Allow users to perform authorized tasks pertaining to data and system administration responsibilities.

Compatibility Role Name	Authorized Tasks Supported
SYS_AUTH_SSO_ROLE	Allow users to perform authorized tasks pertaining to security and access control responsibilities.
SYS_AUTH_DBA_ROLE	Allow users to perform all authorized tasks.
SYS_AUTH_BACKUP_ROLE	Allow users to perform all backups.
SYS_AUTH_MULTIPLEX_ADMIN_ROLE	Allow users to perform authorized tasks to manage Multiplex.
SYS_AUTH_OPERATOR_ROLE	Allow users to checkpoint databases, drop connections (including those for users with SYS_AUTH_DBA_ROLE), back up databases, and monitor the system.
SYS_AUTH_PERMS_ADMIN_ROLE	Allow users to manage data privileges, groups, authorities, and passwords.
SYS_AUTH_PROFILE_ROLE	Allow users to enable/disable server tracing for application profiling.
SYS_AUTH_READFILE_ROLE	Allow users to read to a file resident on the server machine.
SYS_AUTH_READCLIENTFILE_ROLE	Allow users to read to a file resident on the client machine.
SYS_AUTH_RESOURCE_ROLE	Allow users to create new database objects, such as tables, views, indexes, or procedures.
SYS_AUTH_SPACE_ADMIN_ROLE	Allow users to manage dbspaces.
SYS_AUTH_USER_ADMIN_ROLE	Allow users to manage external logins, login policies, and other users.
SYS_AUTH_VALIDATE_ROLE	Allow users to validate or check tables, materialized views, indexes or databases in the system store that are owned by any user.
SYS_AUTH_WRITEFILE_ROLE	Allow users to write to a file resident on the server machine.
SYS_AUTH_WRITECLIENTFILE_ROLE	Allow users to write to a file resident on the client machine.

There is a behavior change in Sybase Unwired Platform 16.0 with respect to inheritance, for these compatibility roles only:

- SYS_AUTH_DBA_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_AUTH_RESOURCE_ROLE

- SYS_AUTH_VALIDATE_ROLE only

Prior to 16.0, the default inheritance behavior for these roles was to not allow grantees to automatically inherit the underlying system privileges. As of 16.0, the default behavior is to allow automatic inheritance.

View Grantees of a Compatibility Role

Display a list of the users and roles granted membership to a compatibility role.

Prerequisites

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > Compatibility Roles**.
3. Select a compatibility role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When viewing a list of grantees to a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of grantees granted to the compatibility role along with their corresponding grant option appears.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.

Grant Option	Description
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

See also

- *View Underlying Roles Granted to a Compatibility Role* on page 1058
- *View System Privileges Granted to a Compatibility Role* on page 1059
- *Adding a Grantee to a Compatibility Role* on page 1061
- *Changing a Grantee's Administrative Rights on a Compatibility Role* on page 1063
- *Removing a Grantee from a Compatibility Role* on page 1065
- *Deleting a Compatibility Role* on page 1066
- *Role-Based Compatibility Role Privilege Summary* on page 1067
- *Authenticating a Login Account for a Managed Resource* on page 282

View Underlying Roles Granted to a Compatibility Role

Display a list of the underlying roles granted to a compatibility role.

Prerequisites

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

You cannot modify or remove the underlying roles granted to a compatibility role, but you can add and remove additional underlying roles to the role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > Compatibility Roles**.
3. Select a compatibility role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Roles**, or
 - From the Administration Console menu bar, select **Resource > Manage Roles**.

Warning! When viewing a list of the underlying role of a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the

differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of underlying roles granted to the compatibility role along with their corresponding grant option appears.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

See also

- *View Grantees of a Compatibility Role* on page 1057
- *View System Privileges Granted to a Compatibility Role* on page 1059
- *Adding a Grantee to a Compatibility Role* on page 1061
- *Changing a Grantee's Administrative Rights on a Compatibility Role* on page 1063
- *Removing a Grantee from a Compatibility Role* on page 1065
- *Deleting a Compatibility Role* on page 1066
- *Role-Based Compatibility Role Privilege Summary* on page 1067
- *Authenticating a Login Account for a Managed Resource* on page 282

View System Privileges Granted to a Compatibility Role

Display a list of the system privileges granted to a compatibility role.

Prerequisites

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

You cannot modify or remove the underlying system privilege granted to a compatibility role, but you can add and remove additional system privileges to the role.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > Compatibility Roles**.
3. Select a compatibility role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage System Privileges**, or
 - From the Administration Console menu bar, select **Resource > Manage System Privileges**.

A list of system privileges granted to the compatibility role along with their corresponding grant option appears.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

See also

- *View Grantees of a Compatibility Role* on page 1057
- *View Underlying Roles Granted to a Compatibility Role* on page 1058
- *Adding a Grantee to a Compatibility Role* on page 1061
- *Changing a Grantee's Administrative Rights on a Compatibility Role* on page 1063
- *Removing a Grantee from a Compatibility Role* on page 1065
- *Deleting a Compatibility Role* on page 1066
- *Role-Based Compatibility Role Privilege Summary* on page 1067
- *Authenticating a Login Account for a Managed Resource* on page 282

Adding a Grantee to a Compatibility Role

Add a user or role as a member (grantee) of a compatibility role. Grantee inherits all underlying system privileges and roles of the compatibility role.

Prerequisites

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the compatibility role.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > Compatibility Roles**.
3. Select a compatibility role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When adding a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the compatibility role appears.

4. Click **Grant**.
5. Select one or more user or roles to grant.

Tip: Use **Shift-click** or **Control-click** to select multiple users or roles.

6. Click **OK**.
The new grantees appear with **Role only** rights (no administrative rights).
7. (Optional) To modify the administrative rights, highlight a grantee. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

Note: The following steps represent a behavior change with SAP Sybase IQ 16.0, for the following roles only.

- SYS_AUTH_DBA_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_RUN_REPLICATION_ROLE
- SYS_AUTH_RESOURCE_ROLE
- SYS_AUTH_VALIDATE_ROLE

Prior to 16.0, when granting membership to one of these roles, the default inheritance behavior was to not allow members of the role to automatically inherit the underlying system privileges and roles of the compatibility role. Only the log on user (of the role) would inherit. As of 16.0, the default behavior is to allow automatic inheritance by all members of the role.

-
8. (Optional for SYS_AUTH_DBA_ROLE only) To prevent automatic inheritance of the SYS_AUTH_DBA_ROLE when granted with the **Administrative and Role** option, click in the Inheritance column, and select No Inheritance.
 9. (Optional for SYS_AUTH_DBA_ROLE, SYS_AUTH_BACKUP_ROLE, SYS_RUN_REPLICATION_ROLE, SYS_AUTH_RESOURCE_ROLE, or SYS_AUTH_VALIDATE_ROLE only) To prevent automatic inheritance when granted with **Role only** option, click in the Inheritance column, and select No Inheritance.
 10. Click **OK**.

See also

- *View Grantees of a Compatibility Role* on page 1057
- *View Underlying Roles Granted to a Compatibility Role* on page 1058
- *View System Privileges Granted to a Compatibility Role* on page 1059
- *Changing a Grantee's Administrative Rights on a Compatibility Role* on page 1063
- *Removing a Grantee from a Compatibility Role* on page 1065
- *Deleting a Compatibility Role* on page 1066
- *Role-Based Compatibility Role Privilege Summary* on page 1067
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Changing a Grantee's Administrative Rights on a Compatibility Role

Changes a member's (grantee's) ability to manage a compatibility role.

Prerequisites

Database Version	Role-Based Standalone Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> Administrative rights over the role (role administrator). MANAGE ROLES system privilege if the role has a global role administrator.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Compatibility Role**.
3. Select a compatibility role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When modifying the administrative rights of a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the role appears.

4. Highlight a grantee to be modified. Click in the Grant Option column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Role only	(default) Grantee can use the underlying system privileges of the role only.
Administrative only	Grantee can grant and revoke the selected role to other users and roles, but cannot use its underlying system privileges.

Grant Option	Description
Administrative and role	Grantee can grant and revoke the selected role to other users and roles and use its underlying system privileges.

Note: The following steps represent a behavior change with SAP Sybase IQ 16.0, for the following roles only.

- SYS_AUTH_DBA_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_RUN_REPLICATION_ROLE
- SYS_AUTH_RESOURCE_ROLE
- SYS_AUTH_VALIDATE_ROLE

Prior to 16.0, when granting membership to one of these roles, the default inheritance behavior was to not allow members of the role to automatically inherit the underlying system privileges and roles of the compatibility role. Only the log on user (of the role) would inherit. As of 16.0, the default behavior is to allow automatic inheritance by all members of the role.

5. (Optional for SYS_AUTH_DBA_ROLE only) To prevent automatic inheritance of the SYS_AUTH_DBA_ROLE when granted with the **Administrative and Role** option, click in the Inheritance column, and select No Inheritance.
6. (Optional for SYS_AUTH_DBA_ROLE, SYS_AUTH_BACKUP_ROLE, SYS_RUN_REPLICATION_ROLE, SYS_AUTH_RESOURCE_ROLE, or SYS_AUTH_VALIDATE_ROLE only) To prevent automatic inheritance when granted with **Role only** option, click in the Inheritance column, and select No Inheritance.
7. Click **OK**.

See also

- *View Grantees of a Compatibility Role* on page 1057
- *View Underlying Roles Granted to a Compatibility Role* on page 1058
- *View System Privileges Granted to a Compatibility Role* on page 1059
- *Adding a Grantee to a Compatibility Role* on page 1061
- *Removing a Grantee from a Compatibility Role* on page 1065
- *Deleting a Compatibility Role* on page 1066
- *Role-Based Compatibility Role Privilege Summary* on page 1067
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Removing a Grantee from a Compatibility Role

Remove a user or role as a member (grantee) of a compatibility role. Grantees lose the ability to use any underlying system privileges or roles of the compatibility role.

Prerequisites

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the compatibility role.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role-Based > Compatibility Roles**.
3. Select a compatibility role from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

Warning! When removing a grantee which is also a role, be sure you select the correct menu option. Each option has different inheritance outcomes. To review the differences, see *Security Implications of the Managing Grantees and Managing Roles Options*.

A list of users and roles currently granted to the role appears.

4. Highlight a user or role to be removed from the compatibility role and click **Revoke**.

Note: The **Revoke** button is unavailable if you do not have administrative rights to the selected role.

5. Click **OK**.

See also

- *View Grantees of a Compatibility Role* on page 1057
- *View Underlying Roles Granted to a Compatibility Role* on page 1058
- *View System Privileges Granted to a Compatibility Role* on page 1059
- *Adding a Grantee to a Compatibility Role* on page 1061
- *Changing a Grantee's Administrative Rights on a Compatibility Role* on page 1063

- *Deleting a Compatibility Role* on page 1066
- *Role-Based Compatibility Role Privilege Summary* on page 1067
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Security Implications of the Managing Grantees and Managing Roles Options* on page 920

Deleting a Compatibility Role

Delete a compatibility role from the database.

Prerequisites

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the compatibility role being deleted.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

In order to delete a compatibility role, these criteria must be met:

- All of its underlying system privileges must have been granted to at least one user-defined role.
 - No users or roles are currently granted to the role.
1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
 2. In the left pane, select **IQ Servers > Security > Role Based > Compatibility Roles**.
 3. Select a compatibility role from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.
 4. Select one or more compatibility roles from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple compatibility roles.

5. (Optional) Select **Revoke role permissions** to remove any users and roles currently granted to the compatibility role.

Note: A compatibility role cannot be deleted if any members are currently granted.

6. Click Yes.

See also

- *View Grantees of a Compatibility Role* on page 1057
- *View Underlying Roles Granted to a Compatibility Role* on page 1058
- *View System Privileges Granted to a Compatibility Role* on page 1059
- *Adding a Grantee to a Compatibility Role* on page 1061
- *Changing a Grantee's Administrative Rights on a Compatibility Role* on page 1063
- *Removing a Grantee from a Compatibility Role* on page 1065
- *Role-Based Compatibility Role Privilege Summary* on page 1067
- *Authenticating a Login Account for a Managed Resource* on page 282

Role-Based Compatibility Role Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based compatibility role tasks.

View Grantees, Underlying Roles, and System Privileges Granted to a Compatibility Role

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Granting and Revoking a Grantee to and from a Compatibility Roles

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the compatibility role.

Deleting Compatibility Roles

Database Version	Role-Based Compatibility Role Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over the compatibility role being deleted.

See also

- *View Grantees of a Compatibility Role* on page 1057

- *View Underlying Roles Granted to a Compatibility Role* on page 1058
- *View System Privileges Granted to a Compatibility Role* on page 1059
- *Adding a Grantee to a Compatibility Role* on page 1061
- *Changing a Grantee's Administrative Rights on a Compatibility Role* on page 1063
- *Removing a Grantee from a Compatibility Role* on page 1065
- *Deleting a Compatibility Role* on page 1066

System Privileges

System privileges control the rights of users to perform authorized database tasks.

You can grant and revoke system privileges to users and roles, with or without administrative rights, but you cannot delete them.

View Grantees of a System Privilege

Display a list of the users and roles granted to a system privilege.

Prerequisites

Database Version	Role-Based System Privilege Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > System Privileges**.
3. Select a system privilege from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

A list of grantees granted to the system privilege along with their corresponding grant option appears.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

See also

- *Adding a Grantee to a System Privilege* on page 1069
- *Changing a Grantee's Administrative Rights on a System Privilege* on page 1071
- *Removing a Grantee from a System Privilege* on page 1072
- *Role-Based System Privilege Privilege Summary* on page 1073
- *System Privileges Listed by Functional Area* on page 1074
- *List All System Privileges* on page 1106
- *Authenticating a Login Account for a Managed Resource* on page 282

Adding a Grantee to a System Privilege

Add users or roles to a system privilege grant list.

Prerequisites

Database Version	Role-Based System Privilege Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over any system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > System Privileges**.

3. Select a system privilege from the right pane and either:

- Click the arrow to the right of the name and select **Manage Grantees**, or
- From the Administration Console menu bar, select **Resource > Manage Grantees**.

A list of users and roles currently granted the system privilege appears.

4. Click **Grant**.

5. Select one or more users or roles.

Tip: Use **Shift-click** or **Control-click** to select multiple users or roles.

6. Click **OK**.

The new grantees appear granted with **Privilege only** rights (no administrative rights).

7. Optional) To modify the administrative rights, highlight a grantee. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

8. Click **OK**.

See also

- *View Grantees of a System Privilege* on page 1068
- *Changing a Grantee's Administrative Rights on a System Privilege* on page 1071
- *Removing a Grantee from a System Privilege* on page 1072
- *Role-Based System Privilege Privilege Summary* on page 1073
- *System Privileges Listed by Functional Area* on page 1074
- *List All System Privileges* on page 1106
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing a Grantee's Administrative Rights on a System Privilege

Change a user or role's ability to manage a system privilege.

Prerequisites

Database Version	Role-Based System Privilege Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over any system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > System Privileges**.
3. Select a system privilege from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

A list of users and roles currently granted to the system privilege appears.

4. Highlight a grantee to be modified. Click in the Grant Options column, click the arrow, and select the administrative rights to be granted.

Grant Option	Description
Privilege only	(default) Grantees can perform authorized tasks requiring the selected privilege, but cannot grant the system privilege to other users and roles.
Administrative only	Grantees can grant and revoke the selected system privilege to other users and roles, but cannot perform authorized tasks requiring the selected system privilege.
Administrative and privilege	Grantees can grant and revoke the selected system privilege to other users and roles and can perform authorized tasks requiring the selected system privilege.

5. Click **OK**.

See also

- *View Grantees of a System Privilege* on page 1068
- *Adding a Grantee to a System Privilege* on page 1069
- *Removing a Grantee from a System Privilege* on page 1072
- *Role-Based System Privilege Privilege Summary* on page 1073
- *System Privileges Listed by Functional Area* on page 1074
- *List All System Privileges* on page 1106
- *Authenticating a Login Account for a Managed Resource* on page 282

Removing a Grantee from a System Privilege

Remove a user or role as a member (grantee) of a system privilege grant list.

Prerequisites

Database Version	Role-Based System Privilege Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over any system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The selected resource supports role-based security

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Role Based > System Privileges**.
3. Select a system privilege from the right pane and either:
 - Click the arrow to the right of the name and select **Manage Grantees**, or
 - From the Administration Console menu bar, select **Resource > Manage Grantees**.

A list of users and roles currently granted to the system privilege appears.

4. Highlight a user or role to be removed and click **Revoke**.

Note: The **Revoke** button is unavailable if you do not have administrative rights to the selected system privilege.

5. Click **OK**.

See also

- *View Grantees of a System Privilege* on page 1068
- *Adding a Grantee to a System Privilege* on page 1069

- *Changing a Grantee's Administrative Rights on a System Privilege* on page 1071
- *Role-Based System Privilege Privilege Summary* on page 1073
- *System Privileges Listed by Functional Area* on page 1074
- *List All System Privileges* on page 1106
- *Authenticating a Login Account for a Managed Resource* on page 282

Role-Based System Privilege Privilege Summary

A list of the system privileges and object permissions required to complete the various role-based system privilege tasks.

View Users and Roles Granted to a System Privilege

Database Version	Role-Based System Privilege Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Adding and Removing Grantees to and From a System Privilege

Database Version	Role-Based System Privilege Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over any system privilege.

Changing Administrative Rights of a Grantee of a System Privilege

Database Version	Role-Based System Privilege Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires administrative rights over any system privilege.

See also

- *View Grantees of a System Privilege* on page 1068
- *Adding a Grantee to a System Privilege* on page 1069
- *Changing a Grantee's Administrative Rights on a System Privilege* on page 1071
- *Removing a Grantee from a System Privilege* on page 1072
- *System Privileges Listed by Functional Area* on page 1074
- *List All System Privileges* on page 1106

System Privileges Listed by Functional Area

A list of system privileges organized by functional area.

See also

- *View Grantees of a System Privilege* on page 1068
- *Adding a Grantee to a System Privilege* on page 1069
- *Changing a Grantee's Administrative Rights on a System Privilege* on page 1071
- *Removing a Grantee from a System Privilege* on page 1072
- *Role-Based System Privilege Privilege Summary* on page 1073
- *List All System Privileges* on page 1106

Database System Privileges

System privileges pertaining to performing authorized tasks on databases.

See also

- *List All System Privileges* on page 1106

ALTER DATABASE System Privilege

Required to alter a database.

The ALTER DATABASE system privilege allows a user to:

- Perform a database upgrade
- Perform cost model calibration
- Load statistics
- Change transaction logs (also requires the SERVER OPERATOR system privilege)
- Change ownership of the database (also requires the MANAGE ANY MIRROR SERVER system privilege)

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

BACKUP DATABASE System Privilege

Allows a user to back up a database on one or more archive devices.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CHECKPOINT System Privilege

Required to force the database server to execute a checkpoint.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DROP CONNECTION System Privilege

Required to drop any user connections to the database.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

MANAGE PROFILING System Privilege

Required to enable or disable server tracing for application profiling. The DIAGNOSTICS system role is also required to fully utilize diagnostics functionality for user information.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

MONITOR System Privilege

Required to allow a user to perform monitoring related tasks such as access privileged statistics, run server monitor related procedures, and so on.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Database Options System Privileges

System privileges pertaining to performing authorized tasks to set database options.

See also

- *List All System Privileges* on page 1106

SET ANY PUBLIC OPTION System Privilege

Required to set any PUBLIC system database option that does not require the SET ANY SECURITY OPTION or SET ANY SYSTEM OPTION system privileges.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

SET ANY SECURITY OPTION System Privilege

Required to set any PUBLIC security database options.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

SET ANY SYSTEM OPTION System Privilege

Required to set any PUBLIC system database options.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

SET ANY USER DEFINED OPTION System Privilege

Required to set any user-defined options.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Data Type System Privileges

System privileges pertaining to performing authorized tasks on data types.

See also

- *List All System Privileges* on page 1106

ALTER DATATYPE System Privilege

Required to alter data types.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE DATATYPE System Privilege

Required to create data types.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DROP DATATYPE System Privilege

Required to drop data types.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Dbspaces System Privileges

System privileges pertaining to performing authorized tasks on dbspaces.

See also

- *List All System Privileges* on page 1106

MANAGE ANY DBSPACE System Privilege

Required to perform management-related tasks on dbspaces.

The MANAGE ANY DBSPACE system privilege allows a user to:

- Issue CREATE, ALTER, DROP, or COMMENT statements on any dbspace
- GRANT or REVOKE the CREATE object-level privilege on any dbspace
- Move data to any dbspace
- Issue a read-only selective restore statement on any dbspace
- Run the database delete file function

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Debugging System Privileges

System privileges pertaining to performing authorized tasks related to debugging.

See also

- *List All System Privileges* on page 1106

DEBUG ANY PROCEDURE System Privilege

Required to debug all code in any database object.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Events System Privileges

System privileges pertaining to authorized tasks on events.

See also

- *List All System Privileges* on page 1106

MANAGE ANY EVENT System Privilege

Required to create, alter, drop or trigger events.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

External Environment System Privileges

System privileges pertaining to performing authorized tasks on external environments.

See also

- *List All System Privileges* on page 1106

CREATE EXTERNAL REFERENCE System Privilege

Required to create external references in the database.

This system privilege is required in addition to any other system privileges required for creating a database object that references an external object.

For example:

- To create an external term breaker or a self-owned text configuration that uses an external term breaker requires the system privilege CREATE TEXT CONFIGURATION in addition to the CREATE EXTERNAL REFERENCE system privilege.
- To create an external procedure or function requires the CREATE PROCEDURE system privilege in addition to the CREATE EXTERNAL REFERENCE system privilege.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

MANAGE ANY EXTERNAL ENVIRONMENT System Privilege

Required to manage external environments.

The MANAGE ANY EXTERNAL ENVIRONMENT system privilege allows a user to:

- Issue ALTER or COMMENT statements on an external environment
- Issue START or STOP statements on an external environment

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

MANAGE ANY EXTERNAL OBJECT System Privilege

Required to issue install, comment on, or remove external objects.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Files System Privileges

System privileges pertaining to authorized tasks for files.

See also

- *List All System Privileges* on page 1106

READ CLIENT FILE System Privilege

Required to read a file resident on the client machine.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

READ FILE System Privilege

Required to read a file resident on the server machine.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

WRITE CLIENT FILE System Privilege

Required to write a file resident on the client machine.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

WRITE FILE System Privilege

Required to write a file resident on the server machine.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Indexes System Privileges

System privileges pertaining to authorized tasks for indexes.

See also

- *List All System Privileges* on page 1106

ALTER ANY INDEX System Privilege

Required to alter an existing index.

The ALTER ANY INDEX system privilege allows a user to:

- Alter indexes on any table owned by any user
- Issue COMMENT statement on any index owned by any user

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE ANY INDEX System Privilege

Required to create a new index.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

The CREATE ANY INDEX system privilege allows a user to:

- Create indexes on any table owned by any user
- Issue COMMENT statement on any index owned by any user

See also

- *List All System Privileges* on page 1106

DROP ANY INDEX System Privilege

Required to drop indexes on any table owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

LDAP System Privileges

System privileges pertaining to performing authorized tasks on an LDAP server configuration object.

See also

- *List All System Privileges* on page 1106

MANAGE ANY LDAP SERVER System Privilege

Required to issue CREATE, ALTER, or DROP statements on an LDAP server configuration object.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Materialized Views System Privileges

System privileges pertaining to performing authorized tasks on materialized views.

See also

- *List All System Privileges* on page 1106

CREATE ANY MATERIALIZED VIEW System Privilege

Required to create materialized views that are owned by any user. It also allows users to issue the COMMENT statement on materialized views owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE MATERIALIZED VIEW System Privilege

Required to create self-owned materialized views. It also allows users to issue the COMMENT statement on self-owned materialized views.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

ALTER ANY MATERIALIZED VIEW System Privilege

Required to alter materialized views owned by any user. It also allows users to issue the COMMENT statement on materialized views owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DROP ANY MATERIALIZED VIEW System Privilege

Required to drop materialized views owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Messages System Privileges

System privileges pertaining to performing authorized tasks for messages.

See also

- *List All System Privileges* on page 1106

CREATE MESSAGE System Privilege

Required to create messages.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DROP MESSAGE System Privilege

Required to drop messages.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Miscellaneous System Privileges

System privileges pertaining to performing miscellaneous authorized tasks.

See also

- *List All System Privileges* on page 1106

ALTER ANY OBJECT System Privilege

Required to alter an object owned by anyone.

The ALTER ANY OBJECT system privilege allows a user to issue these statements:

- ALTER TABLE
- ALTER INDEX
- ALTER JOIN INDEX
- ALTER VIEW
- ALTER MATERIALIZED VIEW
- ALTER PROCEDURE
- ALTER EVENT
- ALTER SEQUENCE
- ALTER FUNCTION
- ALTER DATATYPE
- ALTER MESSAGE
- ALTER TEXT CONFIGURATION
- ALTER TRIGGER
- ALTER STATISTICS
- COMMENT on different objects
- ALTER SPATIAL REFERENCE SYSTEM
- ALTER SPATIAL UNIT OF MEASURE

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

ALTER ANY OBJECT OWNER System Privilege

Required to change the owner of a user table owned by anyone.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

Note: This system privilege applies to table objects only. Owners of other objects, such as procedures, materialized views, etc., cannot be changed.

See also

- *List All System Privileges* on page 1106

COMMENT ANY OBJECT System Privilege

Required to comment on any object owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE ANY OBJECT System Privilege

Required to create an object owned by anyone.

The CREATE ANY OBJECT system privilege allows a user to issue these statements:

- COMMENT on different objects
- CREATE DATATYPE
- CREATE EVENT
- CREATE FUNCTION
- CREATE INDEX
- CREATE JOIN INDEX
- CREATE MATERIALIZED VIEW
- CREATE MESSAGE
- CREATE PROCEDURE
- CREATE SCHEMA
- CREATE SEQUENCE
- CREATE SPATIAL REFERENCE SYSTEM
- CREATE SPATIAL UNIT OF MEASURE
- CREATE STATISTICS
- CREATE TABLE
- CREATE TEXT CONFIGURATION
- CREATE VIEW

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DROP ANY OBJECT System Privilege

Required to drop an object owned by anyone.

The DROP ANY OBJECT system privilege allows a user to issue these statements:

- DROP DATATYPE
- DROP EVENT
- DROP FUNCTION
- DROP INDEX
- DROP JOIN INDEX
- DROP MATERIALIZED VIEW
- DROP MESSAGE
- DROP PROCEDURE
- DROP SEQUENCE
- DROP SPATIAL REFERENCE SYSTEM
- DROP SPATIAL UNIT OF MEASURE
- DROP STATISTICS
- DROP TABLE
- DROP TEXT CONFIGURATION
- DROP TRIGGER
- DROP VIEW

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

MANAGE ANY OBJECT PRIVILEGES System Privilege

Required to manage objects.

The MANAGE ANY OBJECT PRIVILEGES system privilege allows a user to perform management-related tasks such as:

- Grant any object-level privilege (INSERT, UPDATE, DELETE, SELECT, ALTER, REFERENCES or EXECUTE) on objects owned by any user
- Revoke any object-level privilege granted by the object owner or another user with MANAGE ANY OBJECT PRIVILEGES system privilege

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

REORGANIZE ANY OBJECT System Privilege

Required to issue the REORGANIZE statement on applicable objects owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

VALIDATE ANY OBJECT System Privilege

Required to validate or check tables, materialized views, indexes or databases in the system store owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Mirror Server System Privileges

System privileges pertaining to authorized tasks for mirrored servers.

See also

- *List All System Privileges* on page 1106

MANAGE ANY MIRROR SERVER System Privilege

Required to perform high availability server administrative tasks.

The MANAGE ANY MIRROR SERVER system privilege allows a user to:

- Issue CREATE, ALTER or DROP statement on mirrored servers
- Change mirror server parameters
- Set options on mirror servers
- Execute the ALTER statement to change ownership of a database

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Multiplex System Privileges

Two specific system privileges are required to perform authorized tasks in a multiplex environment.

See also

- *List All System Privileges* on page 1106

ACCESS SERVER LS System Privilege

Allows logical server connection using the SERVER logical server context.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

MANAGE MULTIPLEX System Privilege

Allows administrative tasks related to multiplex server management.

The MANAGE MULTIPLEX system privilege allows a user to:

- Issue multiplex-related CREATE, ALTER, DROP, or COMMENT statements on logical server policies
- Issue multiplex-related CREATE, ALTER, DROP, or COMMENT statements on logical servers
- Perform exclusive assignment of a dbspace to logical servers
- Release a populated dbspace from the exclusive use of a logical server

Note: The MANAGE MULTIPLEX system privilege also manages failover configurations, and is required for a manual failover.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Procedures System Privileges

System privileges pertaining to performing authorized tasks for procedures.

See also

- *List All System Privileges* on page 1106

ALTER ANY PROCEDURE System Privilege

Required to alter any stored procedure or function owned by any user.

The ALTER ANY PROCEDURE system privilege allows a user to:

- Alter stored procedures and functions owned by any user
- Issue COMMENT statement on procedures owned by any user

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE ANY PROCEDURE System Privilege

Required to create any stored procedure or function owned by any user.

The CREATE ANY PROCEDURE system privilege allows a user to:

- Create stored procedures and functions owned by any user
- Issue COMMENT statement on procedures owned by any user

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE PROCEDURE System Privilege

Required to create a self-owned stored procedure or function.

The CREATE PROCEDURE system privilege allows a user to:

- Create self-owned stored procedures and functions
- Issue COMMENT statement on self-owned procedures

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DROP ANY PROCEDURE System Privilege

Required to drop any stored procedure or function owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

EXECUTE ANY PROCEDURE System Privilege

System privilege required to execute any stored procedure or function owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

MANAGE AUDITING System Privilege

Required to run the **sa_audit_string** stored procedure.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Replication System Privileges

System privileges pertaining to performing authorized replication tasks.

See also

- *List All System Privileges* on page 1106

MANAGE REPLICATION System Privilege

System privilege required to perform replication-related tasks.

The MANAGE REPLICATION system privilege allows a user to:

- Issue CREATE, ALTER, DROP, or COMMENT PUBLICATION statement
- Issue CREATE, ALTER, DROP, or SYNCHRONIZATION SUBSCRIPTION statement
- Issue CREATE, ALTER, DROP, or SYNCHRONIZATION USER statement

- Issue CREATE, ALTER, DROP, or COMMENT SYNCHRONIZATION PROFILE statement
- Issue CREATE or DROP SUBSCRIPTION statement
- Issue CREATE REMOTE MESSAGE TYPE statement
- Issue DROP REMOTE MESSAGE TYPE statement
- Issue GRANT or REVOKE CONSOLIDATE statement
- Issue GRANT or REVOKE REMOTE statement
- Issue GRANT or REVOKE PUBLISH statement
- Issue LOCK FEATURE statement
- Issue START, STOP, or SYNCHRONIZE SUBSCRIPTION statement
- Issue PASSSTHROUGH statement
- Issue REMOTE RESET statement
- Issue SET REMOTE OPTION statement
- Issue START or STOP SYNCHRONIZATION SCHEMA CHANGE statement
- Issue SYNCHRONIZE PROFILE statement
- Execute SA_SETREMOTEUSER
- Execute SA_SETSUBSCRIPTION

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Roles System Privileges

System privileges pertaining to performing authorized tasks for roles.

See also

- *List All System Privileges* on page 1106

MANAGE ROLES System Privilege

Required to create new roles and act as the default administrator of roles.

While the MANAGE ROLES system privilege allows a user to create a new user-defined role, it does not allow them to delete the role. For this, a user requires administrative rights on the role.

Users granted the MANAGE ROLES system privilege serve as default global role administrators on a user-defined role.

If no role administrator is specified during the role creation process, the MANAGE ROLES system privilege (SYS_MANAGE_ROLES_ROLE) is automatically granted to the role with the ADMIN ONLY OPTION clause, which allows the global role administrator to administer

the role. If at least one role administrator is specified during the creation process, the `MANAGE ROLES` system privilege is not granted to the role, and global role administrators will be unable to manage the role.

`MANAGE ROLES` is the only system privilege with the ability to be granted the ability to administer user-defined roles.

Note: Administration of a role can also be granted directly to users either during the creation of the role or after the fact. When granted directly to a user, the user does not require the `MANAGE ROLES` system privilege to administer the role.

See also

- *List All System Privileges* on page 1106

UPGRADE ROLE System Privilege

Required to administrate new system privileges introduced when upgrading from a database earlier than 16.0.

By default, the `UPGRADE ROLE` system privilege is granted to the `SYS_AUTH_SA_ROLE` role (if it still exists).

Grant this system privilege using the `WITH ADMIN OPTION`, `WITH NO ADMIN OPTION`, or `WITH ADMIN ONLY OPTION` clause. If you do not specify a clause, the `WITH NO ADMIN OPTION` clause is used by default.

See also

- *List All System Privileges* on page 1106

Sequences System Privileges

System privileges pertaining to performing authorized tasks for sequencing.

See also

- *List All System Privileges* on page 1106

ALTER ANY SEQUENCE System Privilege

Required to alter any sequence.

Grant this system privilege using the `WITH ADMIN OPTION`, `WITH NO ADMIN OPTION`, or `WITH ADMIN ONLY OPTION` clause. If you do not specify a clause, the `WITH NO ADMIN OPTION` clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE ANY SEQUENCE System Privilege

Required to create any sequence.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DROP ANY SEQUENCE System Privilege

Required to drop any sequence.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

USE ANY SEQUENCE System Privilege

Required to use any sequence.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Server Operator System Privileges

System privileges pertaining to performing authorized server operator tasks.

See also

- *List All System Privileges* on page 1106

SERVER OPERATOR System Privilege

Required to perform server-operator-related tasks.

The SERVER OPERATOR system privilege allows a user to:

- Create databases
- Cache management
- Drop databases

- Start or stop a database
- Start or stop a database engine
- Create, alter, or drop a server
- Create encrypted or decrypted databases
- Create encrypted or decrypted files
- Issue ALTER statement to change transaction logs on a database
- Issue RESTORE statement for a full database restore or to restore the catalog only

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Spatial Objects System Privileges

System privileges pertaining to performing authorized tasks on spatial objects.

See also

- *List All System Privileges* on page 1106

MANAGE ANY SPATIAL OBJECT System Privilege

Required to manage any spatial objects.

The MANAGE ANY SPATIAL OBJECT system privilege allows a user to issue:

- Issue CREATE, ALTER, or DROP statements on spatial objects
- Issue CREATE, ALTER, or DROP statements on spatial units of measure
- Issue COMMENT statement on spatial units of measure.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Statistics System Privileges

System privileges pertaining to performing authorized tasks on statistics.

See also

- *List All System Privileges* on page 1106

MANAGE ANY STATISTICS System Privilege

Required to issue CREATE, ALTER, DROP, or UPDATE statements on statistics for any table.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Tables System Privileges

System privileges pertaining to performing authorized tasks on tables.

See also

- *List All System Privileges* on page 1106

ALTER ANY TABLE System Privilege

Required to alter any table owned by anyone.

The ALTER DATABASE system privilege allows a user to:

- Issue ALTER or TRUNCATE statement on tables, table partitions, or views owned by any user
- Issue COMMENT statement on tables owned by any user
- Issue COMMENT statement on columns on tables owned by any user

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE ANY TABLE System Privilege

Required to create tables owned by any user.

The CREATE ANY TABLE system privilege allows a user to:

- Create tables, including proxy tables, owned by any user
- Issue COMMENT statement on tables owned by any user
- Issue COMMENT statement on columns on tables owned by any user

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE PROXY TABLE System Privilege

Required to create self owned proxy tables.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE TABLE System Privilege

Required to create self owned tables.

The CREATE TABLE system privilege allows a user to:

- Create self-owned tables except proxy tables
- Issue COMMENT statement on self-owned tables
- Issue COMMENT statement on columns on self-owned tables

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DELETE ANY TABLE System Privilege

Required to delete rows from tables, table partitions, or views owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DROP ANY TABLE System Privilege

Required to drop tables owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

INSERT ANY TABLE System Privilege

Required to insert rows into tables and views owned by anyone.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

LOAD ANY TABLE System Privilege

Required to execute LOAD command for any table where the **-gl** server switch is set to DBA.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

SELECT ANY TABLE System Privilege

Required to query tables, views, or materialized views owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

TRUNCATE ANY TABLE System Privilege

Required to execute TRUNCATE command for any table.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

UPDATE ANY TABLE System Privilege

Required to update rows in tables and views owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Text Configurations System Privileges

System privileges pertaining to performing authorized task on text configurations.

See also

- *List All System Privileges* on page 1106

ALTER ANY TEXT CONFIGURATION System Privilege

Required to alter text configurations owned by any user.

The ALTER ANY TEXT CONFIGURATION system privilege allows a user to:

- Issue ALTER statement on text configurations owned by any user
- Issue COMMENT statement on text configuration owned by any user

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE ANY TEXT CONFIGURATION System Privilege

Required to create text configurations owned by other users.

The CREATE ANY TEXT CONFIGURATION system privilege allows a user to:

- Create configurations owned by any user
- Issue COMMENT statement on text configuration owned by any user

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE TEXT CONFIGURATION System Privilege

Required to create self owned text configurations.

The CREATE TEXT CONFIGURATION system privilege allows a user to:

- Create self owned text configurations
- Issue COMMENT statement on self owned text configuration

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DROP ANY TEXT CONFIGURATION System Privilege

Required to drop text configurations owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Triggers System Privileges

System privileges pertaining to performing authorized task on triggers.

See also

- *List All System Privileges* on page 1106

ALTER ANY TRIGGER System Privilege

Required to alter triggers. Users can also issue a COMMENT statement on tables if he or she has the ALTER permission on the table.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE ANY TRIGGER System Privilege

Required to create triggers. Users can also issue a COMMENT statement on tables if he or she has the ALTER permission on the table.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Users and Login Management System Privileges

System privileges pertaining to performing authorized task on users and login policies.

See also

- *List All System Privileges* on page 1106

CHANGE PASSWORD System Privilege

Allows users to manage passwords other than their own.

This system privilege can be limited to allow a user to manage passwords for a specific list of users, to manage passwords for any user granted a specific list of roles, or to manage passwords for any existing database user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

MANAGE ANY LOGIN POLICY System Privilege

Required to manage login policies.

The MANAGE ANY LOGIN POLICY system privilege allows a user to:

- Issue CREATE, ALTER, or DROP statement on login policies
- Issue COMMENT statement on login policies

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

MANAGE ANY USER System Privilege

Required to manage users.

The MANAGE ANY USER system privilege allows a user to:

- Issue CREATE, ALTER, or DROP statement on database users (including assigning initial password)
- Define authentication mechanisms for users (Kerberos, Integrated login)
- Issue CREATE or DROP statement on external logins
- Force password change on next login for any user
- Assign a login policy to any user
- Reset the login policy of any user
- Issue COMMENT statement on users, integrated logins, or Kerberos logins.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

SET USER System Privilege

Required to allow a user to temporarily assume the specific roles and system privileges (impersonate) of another user.

Suppose a user who is responsible for performing a key task is unavailable. A backup user is identified. At a minimum, this backup user must have sufficient privileges to complete the task; however, depending on the nature of the task to be performed, if the backup user has additional privileges not available to the original user, there is the potential for these additional privileges to result in the task completing differently than for the original user. Negate this potential by allowing the backup user to temporarily assume the roles and system privileges

specific to the unavailable user. The backup user "impersonates" the regular user until the key task is finished.

There are two component to the SET USER system privilege. The first component is the SET USER system privilege itself. It is granted by a third party to provide a user with the ability to impersonate another user. The second component is the SETUSER command, which actually impersonate another user. You cannot issue the command to impersonate a user if you have not been granted the privilege to impersonate.

Tip: SET USER is two words when referring to the system privilege, but one word (SETUSER) when referring to the command to actually impersonate another user. You grant the SET USER system privilege, but you issue the SETUSER command to impersonate.

You can limit the granting of the SET USER system privilege to impersonate by allowing users to impersonate:

- Any user in the database
- Any user within a specified list of users
- Any user who is a member of one of the specified roles

For one user to impersonate another user, the grantee (impersonating) user must have been granted at least all of the roles and system privileges, with the same or higher administrative privileges, as those already granted to the target (impersonated) user. The grantee can have been granted additional roles, system privileges, or higher administrative privileges, but not fewer. While a user is impersonating another user, you cannot grant additional privileges to the impersonated user or revoke existing privileges from the impersonating user if doing so invalidate the "at-least" criteria of the SET USER system privilege.

Validation of the at-least criteria occurs when the SETUSER command to impersonate another user is issued, not when the SET USER system privilege is granted to a user. When the SETUSER command is issued, if the grantee fails to meet any of the at-least requirements, a permission denied error message appears.

When one user impersonates another, the user ID of the target user, not the grantee user, is recorded in the audit logs. However, since the act of impersonation (issuance of the SETUSER command) is also recorded in the audit logs, you can determine whether or not a task was executed by the actual user or an impersonating user.

Use the SET USER system privilege only as a temporary measure. While a user is impersonating another user, any roles or system privileges granted to the grantee user are unavailable until the impersonation is terminated. It is strongly recommended that you terminate an impersonation as soon as the required tasks are completed, to allow the grantee to regain their normal roles and system privileges. If you do not deliberately terminate impersonation, it is automatically terminated as soon as the grantee user ends the current session or successfully begins impersonating a different user.

Scenario 1

Assume the following:

- There are two users, User1 and User2.
- There are two roles, Role1 and Role2.
- Role1 has been granted the CREATE TABLE system privilege.
- Role2 has been granted the CREATE ANY TABLE system privilege.
- User1 has been granted Role1.
- User2 has been granted Role1 and Role2.

A task requiring the CREATE TABLES system privilege needs to be performed.

The task is usually performed by User1, who is unavailable. User2 has been identified as the backup user to carry out the task. Since both User1 and User2 have been granted Role1, User2 has the required system privilege to perform the task as himself or herself. However, since User2 has also been granted Role2, which includes higher system privileges with respect to creating tables, there is the potential for the task to complete differently than if performed by User1.

To negate this possibility, User2 can impersonate User1 to complete the task.

Scenario 2 – Meeting At-Least Requirements for Roles

Assume the following:

- There are two users, User1 and User2.
- There are two roles, Role1 and Rol2.
- User1 has been granted Role1.
- User2 has been granted Role1 and Role2.
- User1 has been granted the SET USER system privilege to impersonate User2.
- User2 has been granted the SET USER system privilege to impersonate User1.

User2 can successfully impersonate User1 because they both have been granted Role1, which meets the at-least criteria. However, User1 cannot successfully impersonate User2 because User1 has not been granted Role2 and does not meet the at-least criteria.

Scenario 3 – Meeting At-Least Requirements for Administrative Options

Assume the following:

- There are two users, User4 and User5.
- User4 has been granted Role1 with the WITH ADMIN OPTION clause.
- User5 has been granted Role1 with the WITH NO ADMIN OPTION clause.
- User4 has been granted the SET USER system privilege to impersonate User5.
- User5 has been granted the SET USER system privilege to impersonate User4.

Even though both users have been granted Role1, User5 cannot successfully impersonate User4 because he or she has fewer administrative rights to Role1 than User4, which fails the at-least requirement. However, User4 can impersonate User5 because he or she has more administrative rights to Role1 than User5, which meets the at-least requirement.

See also

- *List All System Privileges* on page 1106

Views System Privileges

System privileges pertaining to performing authorized tasks on views.

See also

- *List All System Privileges* on page 1106

ALTER ANY VIEW System Privilege

Required to alter views owned by any user.

The ALTER ANY VIEW system privilege allows a user to:

- Alter views owned by any user
- Issue COMMENT statement on views owned by any user

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE ANY VIEW System Privilege

Required to create views owned by any user.

The CREATE ANY VIEW system privilege allows a user to:

- Create views owned by any user
- Issue COMMENT statement on views owned by any user

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

CREATE VIEW System Privilege

Required to create self owned views.

The CREATE VIEW system privilege allows a user to:

- Create self owned views
- Issue COMMENT statement on self owned views

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

DROP ANY VIEW System Privilege

Required to drop a view owned by any user.

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

Web Services System Privileges

System privileges pertaining to performing authorized task on Web services.

See also

- *List All System Privileges* on page 1106

MANAGE ANY WEB SERVICE System Privilege

Required to manage tasks related to Web services.

The MANAGE ANY WEB SERVICE system privilege allows a user to:

- Issue CREATE, ALTER, or DROP statements on Web services
- Issue COMMENT statement on Web services

Grant this system privilege using the WITH ADMIN OPTION, WITH NO ADMIN OPTION, or WITH ADMIN ONLY OPTION clause. If you do not specify a clause, the WITH NO ADMIN OPTION clause is used by default.

See also

- *List All System Privileges* on page 1106

List All System Privileges

List of all system privileges.

System privileges control the rights of users to perform authorized database tasks.

See also

- *View Grantees of a System Privilege* on page 1068

- *Adding a Grantee to a System Privilege* on page 1069
- *Changing a Grantee's Administrative Rights on a System Privilege* on page 1071
- *Removing a Grantee from a System Privilege* on page 1072
- *Role-Based System Privilege Privilege Summary* on page 1073
- *System Privileges Listed by Functional Area* on page 1074
- *ACCESS SERVER LS System Privilege* on page 1089
- *ALTER ANY INDEX System Privilege* on page 1081
- *ALTER ANY MATERIALIZED VIEW System Privilege* on page 1083
- *ALTER ANY OBJECT System Privilege* on page 1085
- *ALTER ANY OBJECT OWNER System Privilege* on page 1085
- *ALTER ANY PROCEDURE System Privilege* on page 1090
- *ALTER ANY SEQUENCE System Privilege* on page 1093
- *ALTER ANY TABLE System Privilege* on page 1096
- *ALTER ANY TEXT CONFIGURATION System Privilege* on page 1099
- *ALTER ANY TRIGGER System Privilege* on page 1101
- *ALTER ANY VIEW System Privilege* on page 1105
- *ALTER DATABASE System Privilege* on page 1074
- *ALTER DATATYPE System Privilege* on page 1077
- *BACKUP DATABASE System Privilege* on page 1074
- *CHANGE PASSWORD System Privilege* on page 1101
- *CHECKPOINT System Privilege* on page 1075
- *COMMENT ANY OBJECT System Privilege* on page 1086
- *CREATE ANY INDEX System Privilege* on page 1082
- *CREATE ANY MATERIALIZED VIEW System Privilege* on page 1083
- *CREATE ANY OBJECT System Privilege* on page 1086
- *CREATE ANY PROCEDURE System Privilege* on page 1090
- *CREATE ANY SEQUENCE System Privilege* on page 1094
- *CREATE ANY TABLE System Privilege* on page 1096
- *CREATE ANY TEXT CONFIGURATION System Privilege* on page 1099
- *CREATE ANY TRIGGER System Privilege* on page 1101
- *CREATE ANY VIEW System Privilege* on page 1105
- *CREATE DATATYPE System Privilege* on page 1077
- *CREATE EXTERNAL REFERENCE System Privilege* on page 1079
- *CREATE MATERIALIZED VIEW System Privilege* on page 1083
- *CREATE MESSAGE System Privilege* on page 1084
- *CREATE PROCEDURE System Privilege* on page 1090
- *CREATE PROXY TABLE System Privilege* on page 1097
- *CREATE TABLE System Privilege* on page 1097
- *CREATE TEXT CONFIGURATION System Privilege* on page 1100

- *CREATE VIEW System Privilege* on page 1105
- *DEBUG ANY PROCEDURE System Privilege* on page 1078
- *DELETE ANY TABLE System Privilege* on page 1097
- *DROP ANY INDEX System Privilege* on page 1082
- *DROP ANY MATERIALIZED VIEW System Privilege* on page 1084
- *DROP ANY OBJECT System Privilege* on page 1086
- *DROP ANY PROCEDURE System Privilege* on page 1091
- *DROP ANY SEQUENCE System Privilege* on page 1094
- *DROP ANY TABLE System Privilege* on page 1098
- *DROP ANY TEXT CONFIGURATION System Privilege* on page 1100
- *DROP ANY VIEW System Privilege* on page 1106
- *DROP CONNECTION System Privilege* on page 1075
- *DROP DATATYPE System Privilege* on page 1077
- *DROP MESSAGE System Privilege* on page 1084
- *EXECUTE ANY PROCEDURE System Privilege* on page 1091
- *LOAD ANY TABLE System Privilege* on page 1098
- *INSERT ANY TABLE System Privilege* on page 1098
- *MANAGE ANY DBSPACE System Privilege* on page 1078
- *MANAGE ANY EVENT System Privilege* on page 1079
- *MANAGE ANY EXTERNAL ENVIRONMENT System Privilege* on page 1079
- *MANAGE ANY EXTERNAL OBJECT System Privilege* on page 1080
- *MANAGE ANY LDAP SERVER System Privilege* on page 1082
- *MANAGE ANY LOGIN POLICY System Privilege* on page 1102
- *MANAGE ANY MIRROR SERVER System Privilege* on page 1088
- *MANAGE ANY OBJECT PRIVILEGES System Privilege* on page 1087
- *MANAGE ANY SPATIAL OBJECT System Privilege* on page 1095
- *MANAGE ANY STATISTICS System Privilege* on page 1096
- *MANAGE ANY USER System Privilege* on page 1102
- *MANAGE ANY WEB SERVICE System Privilege* on page 1106
- *MANAGE AUDITING System Privilege* on page 1091
- *MANAGE MULTIPLEX System Privilege* on page 1089
- *MANAGE PROFILING System Privilege* on page 1075
- *MANAGE REPLICATION System Privilege* on page 1091
- *MANAGE ROLES System Privilege* on page 1092
- *MONITOR System Privilege* on page 1075
- *READ CLIENT FILE System Privilege* on page 1080
- *READ FILE System Privilege* on page 1080
- *REORGANIZE ANY OBJECT System Privilege* on page 1088
- *SELECT ANY TABLE System Privilege* on page 1098

- *SERVER OPERATOR System Privilege* on page 1094
- *SET ANY PUBLIC OPTION System Privilege* on page 1076
- *SET ANY SECURITY OPTION System Privilege* on page 1076
- *SET ANY SYSTEM OPTION System Privilege* on page 1076
- *SET ANY USER DEFINED OPTION System Privilege* on page 1076
- *SET USER System Privilege* on page 1102
- *TRUNCATE ANY TABLE System Privilege* on page 1099
- *UPDATE ANY TABLE System Privilege* on page 1099
- *UPGRADE ROLE System Privilege* on page 1093
- *USE ANY SEQUENCE System Privilege* on page 1094
- *VALIDATE ANY OBJECT System Privilege* on page 1088
- *WRITE CLIENT FILE System Privilege* on page 1081
- *WRITE FILE System Privilege* on page 1081

Login Mappings

Map a Windows user profile or a Kerberos principal to an existing user in the database to maintain a single user ID for database connections, operating system logins, and network logins.

Creating a Login Mapping

Create a login mapping to allow easier connection to a network server on Windows or a database that uses the Kerberos network authentication protocol.

Prerequisites

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority along with SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege along with one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Advanced Security option (IQ_SECURITY), if mapping a Kerberos principal.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Login Mappings**.
3. Click the arrow next to **Login Mappings** and select **New**.
The Create Login Mapping Wizard appears.
4. On the Welcome page, specify:

Option	Description
Which type of login mapping do you want to create?	From the list, select Kerberos to map a Kerberos principal or Integrated to map a Windows user profile.
Select a resource for which the login mapping will be created.	From the list, select the name of the server.
What do you want to name the login mapping?	Enter a unique name for the new login map; maximum 128 characters.
Which database user do you want to associate with the login mapping?	From the list, select the name of the user.

5. Click **Next** to add a Comment, or **Finish**.
6. On the Comment page, enter an (optional) comment for the login mapping.
7. Click **Finish**.

Note: If you do not have the SELECT ANY TABLE system privilege or SELECT permission on the **SYSLOGINMAP** view, the login mapping is successfully created, but does not appear on the list.

See also

- *Deleting a Login Mapping* on page 1111
- *Generating Login Mapping DDL Commands* on page 1112
- *Viewing Login Mapping Properties* on page 1113
- *Login Mapping Privilege Summary* on page 1114
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Login Mapping

Delete a login mapping for a Windows user profile or a Kerberos principal.

Prerequisites

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority along with SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege along with one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Advanced Security option (IQ_SECURITY), if deleting a login mapping for a Kerberos principal.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Login Mappings**.

Note: If you do not have the SELECT ANY TABLE system privilege or SELECT permission on the **SYSLOGINMAP** view, the list of login mappings is empty.

3. Select one or more login mappings from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple login mappings.

4. Click **Yes** to confirm deletion.

See also

- *Creating a Login Mapping* on page 1109
- *Generating Login Mapping DDL Commands* on page 1112
- *Viewing Login Mapping Properties* on page 1113
- *Login Mapping Privilege Summary* on page 1114
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Login Mapping DDL Commands

Display the data description language SQL code for adding a login mapping to the database. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	Requires SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Advanced Security option (IQ_SECURITY), if mapping a Kerberos principal.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Login Mappings**.

Note: If you do not have the SELECT ANY TABLE system privilege or SELECT permission on the **SYSLOGINMAP** view, the list of login mappings is empty.

3. Select one or more login mappings from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple login mappings.

The DDL view shows the SQL code used to create the selected login mappings.

See also

- *Creating a Login Mapping* on page 1109
- *Deleting a Login Mapping* on page 1111
- *Viewing Login Mapping Properties* on page 1113
- *Login Mapping Privilege Summary* on page 1114
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing Login Mapping Properties

Display the properties for the selected login mapping.

Prerequisites

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View Login Mapping properties – Requires SELECT permission on the SYSLOGINMAP view.</p> <p>Modify Login Mapping comment – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority along with SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	<p>View any login mapping property page – Requires one of:</p> <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view. <p>Modify a login mapping comment –</p> <ul style="list-style-type: none"> • Requires MANAGE ANY USER system privilege along with one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Login Mappings**.

Note: If you do not have the SELECT ANY TABLE system privilege or SELECT permission on the **SYSLOGINMAP** view, the list of login mappings is empty.

3. Select a login mapping from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Login Mapping Properties view appears. You may edit the Comment section, but the rest of the property page is read-only.

4. If you change the comment, click **Apply**, then **OK**.

See also

- *Creating a Login Mapping* on page 1109
- *Deleting a Login Mapping* on page 1111
- *Generating Login Mapping DDL Commands* on page 1112
- *Login Mapping Privilege Summary* on page 1114
- *Authenticating a Login Account for a Managed Resource* on page 282

Login Mapping Privilege Summary

A list of the system privileges and object permissions required to complete the various login mapping tasks.

Creating a Login Mapping

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• USER ADMIN authority along with SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege along with one of: <ul style="list-style-type: none">• SELECT ANY TABLE system privilege.• SELECT permission on the SYSLOGINMAP view.

Deleting a Login Mapping

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• USER ADMIN authority along with SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	Requires MANAGE ANY USER system privilege along with one of: <ul style="list-style-type: none">• SELECT ANY TABLE system privilege.• SELECT permission on the SYSLOGINMAP view.

Generating Login Mapping DDL Commands

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	Requires SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view.

Viewing Login Mapping Properties

Database Version	Login Mapping Privileges
SAP Sybase IQ 15.3 and 15.4	View Login Mapping properties – Requires SELECT permission on the SYSLOGINMAP view. Modify Login Mapping comment – Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority along with SELECT permission on the SYSLOGINMAP view.
SAP Sybase IQ 16.0	View any login mapping property page – Requires one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view. Modify a login mapping comment – <ul style="list-style-type: none"> • Requires MANAGE ANY USER system privilege along with one of: <ul style="list-style-type: none"> • SELECT ANY TABLE system privilege. • SELECT permission on the SYSLOGINMAP view.

See also

- *Creating a Login Mapping* on page 1109
- *Deleting a Login Mapping* on page 1111
- *Generating Login Mapping DDL Commands* on page 1112
- *Viewing Login Mapping Properties* on page 1113

Login Policies

Login policies govern only the rules for user login and are separate from authorities and permissions.

A login policy is a named object in a database that consists of a set of rules that are applied when you create a database connection for a user. All new databases include a root login policy. You can modify the root login policy values, but you cannot delete the policy. Login policies are not inherited through group memberships.

Creating a Login Policy for a Simplex

Create a login policy to define password and login parameters for users connecting to a simplex database.

Prerequisites

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY LOGIN POLICY system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Login Policies**.
3. Click the arrow next to **Login Policies** and select **New**.
The Create Login Policy Wizard appears.
4. On the Login Policy Name page, specify:

Option	Description
Select the server for which the login policy will be created	From the list, select the resource for which the login policy will be created.
What do you want to name the new login policy?	Enter a unique name for the new login policy; maximum 128 characters.

Option	Description
What would you like the comment to be for this login policy.	(Optional) Enter a comment for the login policy.

5. Click **Next**.
6. On the Login Policy Options page, specify:

Note: For each option, if no value is defined in the Value column, the root policy value is used.

Option	Description
Options	<p>Password life time – Number of days the password is valid. The user must reset the password when the lifetime expires. Valid range is 0 - unlimited (default).</p> <p>Password grace time – Number of days before password expiry that users receive warnings that the password is about to expire. Valid range is 0 (default) - unlimited.</p> <p>Password expiry on next login – Whether the user must reset the password at the next login. Valid values are ON and OFF (default).</p> <p>Locked – Whether the user account is locked when maximum number of failed login attempts is exceeded. Valid values are ON and OFF (default).</p> <p>Maximum connections – Number of times the same user can be logged in to the server. Valid range is 0 - unlimited (default).</p> <p>Maximum failed login attempts – Number of failed login attempts before the account is locked. Valid range is 0 - unlimited (default).</p> <p>Maximum days since login – Number of days allowed between logins before the account is locked. Valid range is 0 - unlimited (default).</p> <p>(16.0 only) Auto unlock time – The time period after which locked accounts are automatically unlocked. This option can be defined in any login policy, including the root login policy. Valid range is 0 - unlimited (default).</p> <p>(16.0 only) LDAP primary server – The name of the primary LDAP server configuration object.</p> <p>(16.0 only) LDAP secondary server – The name of the secondary LDAP server configuration object.</p> <p>(16.0 only) LDAP auto fallback period – The time period, in minutes, after which automatic fallback to the primary server is attempted. Valid range is 0 - unlimited. Default is 15 minutes.</p> <p>(16.0 only) LDAP failover to standard authentication – Permits authentication with standard authentication when authentication with the LDAP server fails due to system resources, network outage, connection timeouts, or similar system failures. However, it does not permit an actual authentication failure returned from an LDAP server to fail over to standard authentication. Valid values are ON (default) and OFF.</p>

Option	Description
	<p>(16.0 only) Change password dual control – Requires input from two users, each granted the CHANGE PASSWORD system privilege, to change the password of another user. Valid values are ON and OFF (default).</p> <p>(16.0 only) Default logical server – Sets the logical server if the connection string omits a Logical Server parameter.</p> <ul style="list-style-type: none"> • Name of an existing user-defined logical server • AUTO – value of the default logical server in the root login policy. • COORDINATOR – the current coordinator node • NONE – denies access to any multiplex server. • OPEN – use alone or with the name of a user-defined logical server. Allows access to all multiplex nodes that are not members of any user-defined logical servers. • SERVER – allows access to all of the multiplex nodes, subject to the semantics of the SERVER logical server. <p>(15.3, 15.4 only) DQP Enabled – Enables or disables DQP at the connection level. Default is ON.</p>
Clear All Overridden Values	Clears all override values set.
Restore to IQ Default	Changes all option settings back to default values.

7. Click **Next**.

8. (16.0 only) On the LDAP page, specify:

Option	Description
Enable LDAP user authentication	Select to allow configuration of SAP Sybase IQ LDAP server properties in a login policy.
Primary LDAP server	Specify the name of the primary SAP Sybase IQ LDAP server by name.
Secondary LDAP server	Specify the name of the secondary SAP Sybase IQ LDAP server by name.

Option	Description
Auto failback period	Specify the time period in minutes after which automatic failback to the primary server will be attempted. Valid range is 0 - 2147483647. Default value is 15 minutes.
Failover to standard authentication	Permits authentication with Standard authentication when authentication with the SAP Sybase IQ LDAP server fails due to system resources, network outage, connection timeouts, or similar system failures. However, it does not permit an actual authentication failure returned from an SAP Sybase IQ LDAP server to failover to Standard authentication. Default value is ON.
Record LDAP DN refresh time	At the time this login policy option is created or modified, the current time value is stored with the login policy. This is the timestamp that each user authentication compares against the value found for the user in the ISYSUSER system table. When the value in the login policy is newer than the value defined in ISYSUSER, the search for a user DN is done to refresh the value in ISYSUSER. The value NOW is the only valid value to assign to this policy option. All others result in an error. The value is stored as a string in the server's default format. Regardless of the server's local timezone, the value is stored in Coordinated Universal Time (UTC). Select the option to record the refresh SAP Sybase IQ LDAP server DN time.

9. Click **Finish**.

See also

- *Creating a Login Policy for a Multiplex* on page 1121
- *Deleting a Login Policy* on page 1125
- *Generating Login Policy DLL Command* on page 1126
- *Viewing or Modifying Login Policy Properties* on page 1127
- *Login Policy Privilege Summary* on page 1132
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Login Policy for a Multiplex

Create a login policy to define password and login parameters for users connecting to a multiplex database. Multiplex servers can only be accessed by logical servers, which can be assigned the login policy.

Prerequisites

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY LOGIN POLICY system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Login Policies**.
3. Click the arrow next to **Login Policies** and select **New**.
The Create Login Policy Wizard appears.
4. On the Login Policy Name page, specify:

Option	Description
Select the server for which the login policy will be created	From the list, select the resource for which the login policy will be created.
What do you want to name the new login policy?	Enter a unique name for the new login policy; maximum 128 characters.
What would you like the comment to be for this login policy.	(Optional) Enter a comment for the login policy.

5. Click **Next**.
6. On the Login Policy Options page, specify:

Note: For each option, if no value is defined in the Value column, the root policy value is used.

Option	Description
Options	<p>Password life time – Number of days the password is valid. The user must reset the password when the lifetime expires. Valid range is 0 - unlimited (default).</p> <p>Password grace time – Number of days before password expiry that users receive warnings that the password is about to expire. Valid range is 0 (default) - unlimited.</p> <p>Password expiry on next login – Whether the user must reset the password at the next login. Valid values are ON and OFF (default).</p> <p>Locked – Whether the user account is locked when maximum number of failed login attempts is exceeded. Valid values are ON and OFF (default).</p> <p>Maximum connections – Number of times the same user can be logged in to the server. Valid range is 0 - unlimited (default).</p> <p>Maximum failed login attempts – Number of failed login attempts before the account is locked. Valid range is 0 - unlimited (default).</p> <p>Maximum days since login – Number of days allowed between logins before the account is locked. Valid range is 0 - unlimited (default).</p> <p>(16.0 only) Auto unlock time – The time period after which locked accounts are automatically unlocked. This option can be defined in any login policy, including the root login policy. Valid range is 0 - unlimited (default).</p> <p>(16.0 only) LDAP primary server – The name of the primary LDAP server configuration object.</p> <p>(16.0 only) LDAP secondary server – The name of the secondary LDAP server configuration object.</p> <p>(16.0 only) LDAP auto fallback period – The time period, in minutes, after which automatic fallback to the primary server is attempted. Valid range is 0 - unlimited. Default is 15 minutes.</p> <p>(16.0 only) LDAP failover to standard authentication – Permits authentication with standard authentication when authentication with the LDAP server fails due to system resources, network outage, connection timeouts, or similar system failures. However, it does not permit an actual authentication failure returned from an LDAP server to fail over to standard authentication. Valid values are ON (default) and OFF.</p>

Option	Description
	<p>(16.0 only) Change password dual control – Requires input from two users, each granted the CHANGE PASSWORD system privilege, to change the password of another user. Valid values are ON and OFF (default).</p> <p>(16.0 only) Default logical server – Sets the logical server if the connection string omits a Logical Server parameter.</p> <ul style="list-style-type: none"> • Name of an existing user-defined logical server • AUTO – value of the default logical server in the root login policy. • COORDINATOR – the current coordinator node • NONE – denies access to any multiplex server. • OPEN – use alone or with the name of a user-defined logical server. Allows access to all multiplex nodes that are not members of any user-defined logical servers. • SERVER – allows access to all of the multiplex nodes, subject to the semantics of the SERVER logical server. <p>(15.3, 15.4 only) DQP Enabled – Enables or disables DQP at the connection level. Default is ON.</p>
Clear All Overridden Values	Clears all override values set.
Restore to IQ Default	Changes all option settings back to default values.

7. Click **Next**.

8. On the Logical Server Assignment page, specify:

Option	Description
Assignment Type	<p>CUSTOM – Allows access to user defined logical server(s), including OPEN. Select each logical server assignment to be overridden.</p> <p>DEFAULT – Inherits logical server assignment of ROOT login policy.</p> <p>NONE – Disallows access to any logical server.</p> <p>SERVER – Allows access to every multiplex node. Connection requires ACCESS SERVER LS system privilege.</p>

Option	Description
Assign logical servers to the login policy by selecting the check box	(For CUSTOM only): Select the logical servers to add to the login policy to.

9. Click Next.

10. On the Logical Server Level Option Overrides page, specify:

Option	Description
Select a logical server and specify option overrides	Specifies the value of the Max Conn. (maximum connection) parameter, which overrides the inherited value. <ul style="list-style-type: none"> To set the value, click in the Max Conn. column beside the logical server to be overridden and specify the override value. The valid range is 0 - unlimited (default). To set the value to Unlimited, click in the Max Conn. column, click the arrow, and select Unlimited.

11. Click Next.

12. On the LDAP page, specify:

Option	Description
Enable LDAP user authentication	Select to allow configuration of SAP Sybase IQ LDAP server properties in a login policy.
Primary LDAP server	Specify the name of the primary SAP Sybase IQ LDAP server by name.
Secondary LDAP server	Specify the name of the secondary SAP Sybase IQ LDAP server by name.
Auto failback period	Specify the time period in minutes after which automatic failback to the primary server will be attempted. Valid range is 0 - 2147483647. Default value is 15 minutes.
Failover to standard authentication	Permits authentication with Standard authentication when authentication with the SAP Sybase IQ LDAP server fails due to system resources, network outage, connection timeouts, or similar system failures. However, it does not permit an actual authentication failure returned from an SAP Sybase IQ LDAP server to failover to Standard authentication. Default value is ON.

Option	Description
Record LDAP DN refresh time	At the time this login policy option is created or modified, the current time value is stored with the login policy. This is the timestamp that each user authentication compares against the value found for the user in the ISYSUSER system table. When the value in the login policy is newer than the value defined in ISYSUSER, the search for a user DN is done to refresh the value in ISYSUSER. The value NOW is the only valid value to assign to this policy option. All others result in an error. The value is stored as a string in the server's default format. Regardless of the server's local timezone, the value is stored in Coordinated Universal Time (UTC). Select the option to record the refresh SAP Sybase IQ LDAP server DN time.

13. Click Finish.

See also

- *Creating a Login Policy for a Simplex* on page 1116
- *Deleting a Login Policy* on page 1125
- *Generating Login Policy DLL Command* on page 1126
- *Viewing or Modifying Login Policy Properties* on page 1127
- *Login Policy Privilege Summary* on page 1132
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Login Policy

Delete a login policy for a simplex or multiplex that is not currently assigned to a user. The root login policy cannot be deleted.

Prerequisites

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY LOGIN POLICY system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Login Policies**.
3. Select one or more login policies from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple login policies.

4. Verify that the list of login policies to be deleted is correct and click **Yes**.

See also

- *Creating a Login Policy for a Simplex* on page 1116
- *Creating a Login Policy for a Multiplex* on page 1121
- *Generating Login Policy DLL Command* on page 1126
- *Viewing or Modifying Login Policy Properties* on page 1127
- *Login Policy Privilege Summary* on page 1132
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Login Policy DLL Command

Generate data description language for one or more login policies. The DDL code can be a useful resource and training tool.

Prerequisites

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Login Policies**.
3. Select one or more login policies from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or

- From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple login policies.

The DDL view opens, showing the SQL code used to create the selected login policies.

See also

- *Creating a Login Policy for a Simplex* on page 1116
- *Creating a Login Policy for a Multiplex* on page 1121
- *Deleting a Login Policy* on page 1125
- *Viewing or Modifying Login Policy Properties* on page 1127
- *Login Policy Privilege Summary* on page 1132
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Login Policy Properties

View or change properties of a login policy for a simplex or multiplex.

Prerequisites

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	View any login policy property page – None required. Modify any login policy property – Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	View any login policy property page – None required. Modify any login policy property – Requires MANAGE ANY LOGIN POLICY system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > Login Policies**.
3. Select one or more login policies from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

Tip: Use **Shift-click** or **Control-click** to select multiple LDAP login policies.

The Login Policy Properties view appears.

4. View or modify the properties.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.

Area	Description
General	<p>Password life time – Number of days the password is valid. The user must reset the password when the lifetime expires. Valid range is 0 - unlimited (default).</p> <p>Password grace time – Number of days before password expiry that users receive warnings that the password is about to expire. Valid range is 0 (default) - unlimited.</p> <p>Password expiry on next login – Whether the user must reset the password at the next login. Valid values are ON and OFF (default).</p> <p>Locked – Whether the user account is locked when maximum number of failed login attempts is exceeded. Valid values are ON and OFF (default).</p> <p>Maximum connections – Number of times the same user can be logged in to the server. Valid range is 0 - unlimited (default).</p> <p>Maximum failed login attempts – Number of failed login attempts before the account is locked. Valid range is 0 - unlimited (default).</p> <p>Maximum days since login – Number of days allowed between logins before the account is locked. Valid range is 0 - unlimited (default).</p> <p>Maximum non-DBA connections – The maximum number of concurrent connections that a user without SERVER OPERATOR or DROP CONNECTION system privileges can make. This option is supported only in the root login policy. Valid range is 0 - unlimited (default).</p> <p>(16.0 only) Auto unlock time – The time period after which locked accounts are automatically unlocked. This option can be defined in any login policy, including the root login policy. Valid range is 0 - unlimited (default).</p> <p>(16.0 Root login policy only) Root auto unlock time – The time period after which locked accounts are automatically unlocked. Valid range is 0 - unlimited. Default is 15 minutes.</p> <p>(16.0 only) LDAP primary server – The name of the primary LDAP server configuration object.</p> <p>(16.0 only) LDAP secondary server – The name of the secondary LDAP server configuration object.</p>

Area	Description
	<p>(16.0 only) LDAP auto failback period – The time period, in minutes, after which automatic failback to the primary server is attempted. Valid range is 0 - unlimited. Default is 15 minutes.</p> <p>(16.0 only) LDAP failover to standard authentication – Permits authentication with standard authentication when authentication with the LDAP server fails due to system resources, network outage, connection timeouts, or similar system failures. However, it does not permit an actual authentication failure returned from an LDAP server to fail over to standard authentication. Valid values are ON (default) and OFF.</p> <p>(16.0 only) Change password dual control – Requires input from two users, each granted the CHANGE PASSWORD system privilege, to change the password of another user. Valid values are ON and OFF (default).</p> <p>(16.0 only) Default logical server – Sets the logical server if the connection string omits a Logical Server parameter.</p> <ul style="list-style-type: none"> • Name of an existing user-defined logical server • AUTO – value of the default logical server in the root login policy. • COORDINATOR – the current coordinator node • NONE – denies access to any multiplex server. • OPEN – use alone or with the name of a user-defined logical server. Allows access to all multiplex nodes that are not members of any user-defined logical servers. • SERVER – allows access to all of the multiplex nodes, subject to the semantics of the SERVER logical server. <p>Clear All Overridden Values – Clears all overridden values set.</p> <p>Restore to IQ Default – Changes all option settings back to default values.</p> <p>Comment – A comment for the login policy.</p>

Area	Description
LDAP (16.0 only)	<p>Enable LDAP user authentication – Enables SAP Sybase IQ LDAP user authentication and allows configuration of Sybase IQ LDAP properties.</p> <p>Primary LDAP server – Select the name of the primary SAP Sybase IQ LDAP server from the drop-down list.</p> <p>Secondary LDAP server – Select the name of the secondary SAP Sybase IQ LDAP server from the drop-down list.</p> <p>Auto fallback period – Specify the time period in minutes after which automatic fallback to the primary server will be attempted. Valid range is 0 – 2147483647. Default value is 15 minutes.</p> <p>Failover to standard authentication – Permits authentication with Standard authentication when authentication with the SAP Sybase IQ LDAP server fails due to system resources, network outage, connection timeouts, or similar system failures. However, it does not permit an actual authentication failure returned from an SAP Sybase IQ LDAP server to failover to Standard authentication. Default value is ON.</p> <p>Update LDAP DN refresh time – Updates the current time value associated with the login policy. During user authentication, this value is compared against the corresponding value found for the user in the ISYSUSER system table. If the value in the login policy is newer than the value defined in ISYSUSER, a search for a new user DN is triggered and the ISYSUSER system table is updated.</p>
Logical Server Assignment (Multiplex only)	<p>Assignment Type –</p> <ul style="list-style-type: none"> • Custom – Allows access to user-defined logical server(s), including OPEN. Select each applicable logical server. • Default – Inherits logical server assignment of root login policy. • None – Disallows access to any logical server. • Server – Allows access to every multiplex node. Connection requires ACCESS SERVER LS system privilege.

Area	Description
Logical Server Option Overrides (Multiplex only)	<p>For any login policy EXCEPT root login policy, page available after selecting Custom and Default Assignment Types only.</p> <p>Max Conn. – Click in the Max Conn. column beside the logical server to be overridden and specify the override value. The valid range is 0 – unlimited (default).</p> <p>(15.3, 15.4 only) DQP Enabled – Enables or disables DQP at the connection level. Valid values are ON (default) and OFF.</p>

5. Click **OK**.

See also

- *Creating a Login Policy for a Simplex* on page 1116
- *Creating a Login Policy for a Multiplex* on page 1121
- *Deleting a Login Policy* on page 1125
- *Generating Login Policy DLL Command* on page 1126
- *Login Policy Privilege Summary* on page 1132
- *Authenticating a Login Account for a Managed Resource* on page 282

Login Policy Privilege Summary

A list of the system privileges and object permissions required to complete the various login policy tasks.

Creating a Login Policy for a Simplex or Multiplex

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY LOGIN POLICY system privilege.

Deleting a Login Policy

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.

Database Version	Login Policy Privileges
SAP Sybase IQ 16.0	Requires MANAGE ANY LOGIN POLICY system privilege.

Generating Login Policy DDL Commands

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing Login Policy Properties

Database Version	Login Policy Privileges
SAP Sybase IQ 15.3 and 15.4	View any login policy property page – None required. Modify any login policy property – Requires one of: <ul style="list-style-type: none"> • DBA authority. • USER ADMIN authority.
SAP Sybase IQ 16.0	View any login policy property page – None required. Modify any login policy property – Requires MANAGE ANY LOGIN POLICY system privilege.

See also

- *Creating a Login Policy for a Simplex* on page 1116
- *Creating a Login Policy for a Multiplex* on page 1121
- *Deleting a Login Policy* on page 1125
- *Generating Login Policy DLL Command* on page 1126
- *Viewing or Modifying Login Policy Properties* on page 1127

LDAP Servers

The SAP Sybase IQ LDAP server configuration object allows LDAP user authentication with SAP Sybase IQ.

Note: SAP Sybase IQ LDAP user authentication is only supported with SAP Sybase IQ 16.0

LDAP Server Overview

SAP Sybase IQ uses a configuration object called LDAP server to provide connections between the SAP Sybase IQ server and external LDAP servers.

Despite its name, the SAP Sybase IQ LDAP server is an object that resides on the SAP Sybase IQ server and is NOT an actual server. The LDAP server configuration object's sole function is

to provide a connection to a physical LDAP server to allow LDAP user authentication. Any settings of the LDAP server database configuration object apply solely to the SAP Sybase IQ side of the LDAP user authentication equation. No LDAP server configuration object settings are written to the physical LDAP server.

Note: Any references to LDAP server in the Sybase Control Center user interface refer to the SAP Sybase IQ LDAP server configuration object, not the external physical LDAP server.

See also

- *Creating an LDAP Server Configuration Object* on page 1134
- *Deleting an LDAP Server Configuration Object* on page 1137
- *Activating an LDAP Server Configuration Object* on page 1138
- *Suspending an LDAP Server Configuration Object* on page 1139
- *Refreshing an LDAP Server Configuration Object* on page 1140
- *Validating a User on an External LDAP Server* on page 1141
- *Generating LDAP Server Configuration Object DDL Commands* on page 1142
- *Viewing or Modifying LDAP Server Configuration Object Properties* on page 1143
- *LDAP Server Configuration Object Privilege Summary* on page 1146

Creating an LDAP Server Configuration Object

Create an LDAP server configuration object to enable LDAP user authentication.

Prerequisites

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Advanced Security option (IQ_SECURITY).

Task

Parameters defined during the creation of an LDAP server configuration object are stored in the ISYSLDAPSERVER (system view SYSLDAPSERVER) system table.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > LDAP Servers**.
3. Click the arrow next to **LDAP Servers** and select **New**.

The Create LDAP Server Wizard appears.

4. On the Welcome page, specify:

Option	Description
Select a resource for which the LDAP server will be created	From the list, select the resource for which the LDAP server configuration object will be created.
What do you want to name the new LDAP server?	Enter a unique name for the new LDAP server configuration object; maximum of 128 characters.
Validate LDAP server properties but do not create LDAP server	(Optional) Select to validate the properties defined for the new LDAP server configuration object without actually creating it.
Activate LDAP server after creation	(Optional) Select to activate the new LDAP server configuration object after creation.

Note: The **Validate LDAP server properties but do not create LDAP server** and **Activate LDAP server after creation** options are mutually exclusive. When one is selected, the other becomes unavailable.

5. Click **Next**.
6. On the Search DN page, specify:

Option	Description
Search URL	Specify the host (by name or by IP address), port number, and search to be performed to look up the DN for a given user ID. For example: ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*
Access Account	Enter the distinguished name for a user used to connect to the LDAP server configuration object. For example: cn=iqadmin, cn=Users, dc=mycompany, dc=com
Password	Enter the password for the Access account.
Encrypted	Select if the Access account password is provided in encrypted format.

7. Click **Next**.
8. On the Attributes page, specify:

Option	Description
Authentication URL	Specify the host (by name or by IP address), port number, and search to be performed to look up the DN for a given user ID, or enter NULL.
Connection timeout	Specify the length of time after which the system stops trying to connect to the LDAP server configuration object. Value can be entered in milliseconds, seconds, or minutes. Valid range is between 1-3600000 milliseconds (3600 seconds or 60 minutes). Default value is 10000 milliseconds.
Connection retries	Specify the maximum number of connection retries. Valid range is 1-60. Default value is 3.
Use TLS protocol on LDAP connections	<p>Select to enable TLS protocol on LDAP connections.</p> <hr/> <p>Note: This option is unavailable if the SEARCH or Authentication URL values use ldps://...</p> <hr/>

9. Click **Next**.

10. (Optional) On the Comment page, specify a comment for the LDAP server configuration object.

Note: This option is unavailable when the option **Validate LDAP server properties but do not create LDAP server** is selected.

11. Click **Finish**.

See also

- *LDAP Server Overview* on page 1133
- *Deleting an LDAP Server Configuration Object* on page 1137
- *Activating an LDAP Server Configuration Object* on page 1138
- *Suspending an LDAP Server Configuration Object* on page 1139
- *Refreshing an LDAP Server Configuration Object* on page 1140
- *Validating a User on an External LDAP Server* on page 1141
- *Generating LDAP Server Configuration Object DDL Commands* on page 1142
- *Viewing or Modifying LDAP Server Configuration Object Properties* on page 1143
- *LDAP Server Configuration Object Privilege Summary* on page 1146
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting an LDAP Server Configuration Object

Delete an LDAP server configuration object.

Prerequisites

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The LDAP server configuration object must be in a suspended state.
- The LDAP server configuration object is not referenced in any login policies.
- You are licensed for the Advanced Security option (IQ_SECURITY).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > LDAP Servers**.
3. Select one or more LDAP servers from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple LDAP servers.

4. (Optional) Select **With Suspend** to suspend the LDAP server configuration objects before deletion.

Note: An LDAP server configuration object must have a status of SUSPENDED before it can be deleted.

5. (Optional) Select **Drop all references** to remove all references of the LDAP server configuration objects being deleted from all login policies.

Note: An LDAP server configuration object cannot be deleted if it is referenced in any login policy.

6. Verify that the list of LDAP server configuration objects to be deleted is correct and click **Yes**.

See also

- *LDAP Server Overview* on page 1133
- *Creating an LDAP Server Configuration Object* on page 1134

- *Activating an LDAP Server Configuration Object* on page 1138
- *Suspending an LDAP Server Configuration Object* on page 1139
- *Refreshing an LDAP Server Configuration Object* on page 1140
- *Validating a User on an External LDAP Server* on page 1141
- *Generating LDAP Server Configuration Object DDL Commands* on page 1142
- *Viewing or Modifying LDAP Server Configuration Object Properties* on page 1143
- *LDAP Server Configuration Object Privilege Summary* on page 1146
- *Authenticating a Login Account for a Managed Resource* on page 282

Activating an LDAP Server Configuration Object

Set an LDAP server configuration object to a READY state. The state of the LDAP server configuration object changes to ACTIVE once a user authentication request successfully processes. Multiple LDAP server configuration objects can be activated at the same time.

Prerequisites

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected LDAP server cannot have a status of READY or ACTIVE.
- You are licensed for the Advanced Security option (IQ_SECURITY).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > LDAP Servers**.
3. Select one or more LDAP servers from the right pane and either:
 - Click the arrow to the right of the name and select **Activate**, or
 - From the Administration Console menu bar, select **Resource > Activate**.

Tip: Use **Shift-click** or **Control-click** to select multiple LDAP servers.

4. Verify that the list of LDAP server configuration objects to be activated is correct and click **Yes**.

If activation is successful, the value in the State column beside the LDAP server configuration object changes to READY.

See also

- *LDAP Server Overview* on page 1133
- *Creating an LDAP Server Configuration Object* on page 1134
- *Deleting an LDAP Server Configuration Object* on page 1137
- *Suspending an LDAP Server Configuration Object* on page 1139
- *Refreshing an LDAP Server Configuration Object* on page 1140
- *Validating a User on an External LDAP Server* on page 1141
- *Generating LDAP Server Configuration Object DDL Commands* on page 1142
- *Viewing or Modifying LDAP Server Configuration Object Properties* on page 1143
- *LDAP Server Configuration Object Privilege Summary* on page 1146
- *Authenticating a Login Account for a Managed Resource* on page 282

Suspending an LDAP Server Configuration Object

Put an LDAP server configuration object into maintenance mode. While in maintenance mode, all connections to the LDAP server configuration object are closed and LDAP user authentication is unavailable.

Prerequisites

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- You are licensed for the Advanced Security option (IQ_SECURITY).
- The selected LDAP server cannot have a status of SUSPENDED.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > LDAP Servers**.
3. Select one or more LDAP servers from the right pane and either:
 - Click the arrow to the right of the name and select **Suspend**, or
 - From the Administration Console menu bar, select **Resource > Suspend**.

Tip: Use **Shift-click** or **Control-click** to select multiple LDAP servers.

4. Verify that the list of LDAP server configuration objects to be suspended is correct and click **Yes**.

If suspension is successful, the value in the State column beside the LDAP server configuration object changes to `SUSPENDED`.

See also

- *LDAP Server Overview* on page 1133
- *Creating an LDAP Server Configuration Object* on page 1134
- *Deleting an LDAP Server Configuration Object* on page 1137
- *Activating an LDAP Server Configuration Object* on page 1138
- *Refreshing an LDAP Server Configuration Object* on page 1140
- *Validating a User on an External LDAP Server* on page 1141
- *Generating LDAP Server Configuration Object DDL Commands* on page 1142
- *Viewing or Modifying LDAP Server Configuration Object Properties* on page 1143
- *LDAP Server Configuration Object Privilege Summary* on page 1146
- *Authenticating a Login Account for a Managed Resource* on page 282

Refreshing an LDAP Server Configuration Object

Re-initializes LDAP user authentication on the LDAP server configuration object.

Prerequisites

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires <code>MANAGE ANY LDAP SERVER</code> system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The selected LDAP server must have a status of `READY` or `ACTIVE`.
- You are licensed for the Advanced Security option (`IQ_SECURITY`).

Task

All connections to the LDAP server configuration object are closed and server option values are re-read and applied to any new connections to the LDAP server configuration object or to incoming authentication requests to an SAP Sybase IQ server. This command does not change the state of the LDAP server configuration object and does not change any existing connections from a client to an SAP Sybase IQ server.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > LDAP Servers**.

3. Select one or more LDAP servers from the right pane and either:
 - Click the arrow to the right of the name and select **Refresh**, or
 - From the Administration Console menu bar, select **Resource > Refresh**.

Tip: Use **Shift-click** or **Control-click** to select multiple LDAP servers.

4. Verify that the list of LDAP server configuration objects to be refreshed is correct and click **Yes**.

See also

- *LDAP Server Overview* on page 1133
- *Creating an LDAP Server Configuration Object* on page 1134
- *Deleting an LDAP Server Configuration Object* on page 1137
- *Activating an LDAP Server Configuration Object* on page 1138
- *Suspending an LDAP Server Configuration Object* on page 1139
- *Validating a User on an External LDAP Server* on page 1141
- *Generating LDAP Server Configuration Object DDL Commands* on page 1142
- *Viewing or Modifying LDAP Server Configuration Object Properties* on page 1143
- *LDAP Server Configuration Object Privilege Summary* on page 1146
- *Authenticating a Login Account for a Managed Resource* on page 282

Validating a User on an External LDAP Server

Validate the existence of a specific user on an external LDAP server.

Prerequisites

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Advanced Security option (IQ_SECURITY).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > LDAP Servers**.
3. Select an LDAP server from the right pane and either:

- Click the arrow to the right of the name and select **Validate User**, or
- From the Administration Console menu bar, select **Resource > Validate User**.

Tip: Use **Shift-click** or **Control-click** to select multiple LDAP servers.

4. Specify:

Option	Description
User Name	The userID to be validated.
User DN	The expected user DN.

5. Click **Yes**.

A message appears indicating whether or not validation of the user was successful.

See also

- *LDAP Server Overview* on page 1133
- *Creating an LDAP Server Configuration Object* on page 1134
- *Deleting an LDAP Server Configuration Object* on page 1137
- *Activating an LDAP Server Configuration Object* on page 1138
- *Suspending an LDAP Server Configuration Object* on page 1139
- *Refreshing an LDAP Server Configuration Object* on page 1140
- *Generating LDAP Server Configuration Object DDL Commands* on page 1142
- *Viewing or Modifying LDAP Server Configuration Object Properties* on page 1143
- *LDAP Server Configuration Object Privilege Summary* on page 1146
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating LDAP Server Configuration Object DDL Commands

Generate data description language for one or more LDAP server configuration objects. The DDL code can be a useful resource and training tool.

Prerequisites

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Advanced Security option (IQ_SECURITY).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > LDAP Servers**.
3. Select one or more LDAP servers from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple LDAP servers.

The DDL view opens, showing the SQL code used to create the LDAP Server configuration objects.

See also

- *LDAP Server Overview* on page 1133
- *Creating an LDAP Server Configuration Object* on page 1134
- *Deleting an LDAP Server Configuration Object* on page 1137
- *Activating an LDAP Server Configuration Object* on page 1138
- *Suspending an LDAP Server Configuration Object* on page 1139
- *Refreshing an LDAP Server Configuration Object* on page 1140
- *Validating a User on an External LDAP Server* on page 1141
- *Viewing or Modifying LDAP Server Configuration Object Properties* on page 1143
- *LDAP Server Configuration Object Privilege Summary* on page 1146
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying LDAP Server Configuration Object Properties

View or change properties to an LDAP server configuration object. Any changes to an LDAP server configuration object are applied on subsequent connections. Any connection already started when the change is applied do not reflect the change.

Prerequisites

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	View any LDAP server property page – None Required. Modify any LDAP server property – Requires MANAGE ANY LDAP SERVER system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the Advanced Security option (IQ_SECURITY).

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Security > LDAP Servers**.
3. Select an LDAP server from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The LDAP Server Properties view appears.

4. View or edit the properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	Name —Name of the LDAP server configuration object.
Read-only	State —Current state of the LDAP server configuration object. Valid states include: <ul style="list-style-type: none">• RESET – Indicates that one or more attributes on the LDAP server configuration object have been entered or modified since last activation.• READY – Indicates that the LDAP server configuration object is ready to accept connections.• ACTIVE – Indicates that the LDAP server configuration object has performed at least one successful LDAP user authentication.• FAILED – Indicates that there is a problem connecting to the LDAP server configuration object.• SUSPENDED – Indicates that the LDAP server configuration object is in maintenance mode, and is not available for LDAP user authentication. Last state change —Date and time the LDAP server configuration object state last changed.

Area	Description
Attributes	<p>Search URL—The host (by name or by IP address), port number, and search to be performed to look up the DN for a given user ID. For example: ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*</p> <p>Authentication URL—The host (by name or by IP address), port number, and search to be performed to look up the DN for a given user ID, or enter NULL.</p> <p>Access account—The distinguished name for a user used to connect to the LDAP server configuration object. For example: cn=iqadmin, cn=Users, dc=mycompany, dc=com</p> <p>Password—The password for the Access account.</p> <p>Encrypted—Indicates that the password is provided in encrypted format.</p> <p>Connection timeout—The length of time after which the system stops trying to connect to the LDAP server configuration object. Value can be entered in milliseconds, seconds, or minutes. Valid range is between 1-3600000 milliseconds (3600 seconds or 60 minutes). Default value is 10000 milliseconds.</p> <p>Connection retries—The maximum number of connection retries. Valid range is 1-60. Default value is 3.</p> <p>Use TLS protocol on LDAP connections—Enables the TLS protocol on LDAP connections.</p> <hr/> <p>Note: This option is unavailable if the SEACH URL value specifies ldps://...</p>
Comment	<p>Comment—A text field for adding an optional comment about the LDAP server configuration object.</p>

5. Click **OK**.

See also

- *LDAP Server Overview* on page 1133
- *Creating an LDAP Server Configuration Object* on page 1134
- *Deleting an LDAP Server Configuration Object* on page 1137
- *Activating an LDAP Server Configuration Object* on page 1138
- *Suspending an LDAP Server Configuration Object* on page 1139
- *Refreshing an LDAP Server Configuration Object* on page 1140
- *Validating a User on an External LDAP Server* on page 1141
- *Generating LDAP Server Configuration Object DDL Commands* on page 1142

- *LDAP Server Configuration Object Privilege Summary* on page 1146
- *Authenticating a Login Account for a Managed Resource* on page 282

LDAP Server Configuration Object Privilege Summary

A list of the system privileges and object permissions required to complete the various LDAP server configuration object tasks for SAP Sybase IQ.

Creating an LDAP Server Configuration Object

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

Deleting an LDAP Server Configuration Object

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

Activating, Suspending, and Refreshing an LDAP Server Configuration Object

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

Validating User

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	Requires MANAGE ANY LDAP SERVER system privilege.

Generating LDAP Server Configuration Object DDL Commands

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying LDAP Server Configuration Object Properties

Database Version	LDAP Server Configuration Object Privileges
SAP Sybase IQ 15.3 and 15.4	Not supported.
SAP Sybase IQ 16.0	View any LDAP server property page – None Required. Modify any LDAP server property – Requires MANAGE ANY LDAP SERVER system privilege.

See also

- *LDAP Server Overview* on page 1133
- *Creating an LDAP Server Configuration Object* on page 1134
- *Deleting an LDAP Server Configuration Object* on page 1137
- *Activating an LDAP Server Configuration Object* on page 1138
- *Suspending an LDAP Server Configuration Object* on page 1139
- *Refreshing an LDAP Server Configuration Object* on page 1140
- *Validating a User on an External LDAP Server* on page 1141
- *Generating LDAP Server Configuration Object DDL Commands* on page 1142
- *Viewing or Modifying LDAP Server Configuration Object Properties* on page 1143

Dbspaces

Add, modify, view properties, or delete a dbspace.

Creating a Dbspace

Add a new dbspace to the database.

Prerequisites

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Space Management > Dbspaces**.
3. Click the arrow next to **Dbspaces** and select **New**.
4. On the General Details page, specify:

Option	Description
Resource	From the list, select the resource for which the dbspace will be created.
Name of dbspace to create	A unique name for the new dbspace.

Option	Description
Store	The store in which to create the new dbspace: Catalog (for IQ metadata), IQ Main (for IQ user data) or RLV (Row-Level Versioning store for in-memory data). Note: Only one dbspace can be created in the RLV store. RLV is applicable in IQ 16.0 for a simplex resource.
Striping	Enables or disables disk striping for this dbspace.
Stripe size (Kb)	The number of kilobytes (KB) to write to each file before the disk-striping algorithm moves to the next stripe for this dbspace. Default value is 1.

5. Click **Next**.
6. On the DB Files page, click **Add** to add files to the dbspace.
7. In the DB File Details view, specify:

Option	Description
Logical name	User-defined name of the DB file.
Path to physical file on disk	Path to the physical file on disk. It is usually best to use an absolute path. A relative path works for simplex servers and for multiplexes that use the SCC shared-disk facility and have the SCC installation directory mounted in the same location on each multiplex server host. If you specify a relative path for a simplex that is later converted to a multiplex, the relative path might cause an error.
Raw device	A check mark indicates the file is on a raw device.
File Size	Space you allocate to the DB file in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB). Unavailable on raw devices; required if the file is not on a raw device. Minimum file size is 8 MB.
Reserve size	Specify a reserve size value and units: kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).

8. Click **OK** to add the file.
9. Click **Finish**.

See also

- *Deleting (Dropping) a Dbspace* on page 1150
- *Preallocating Space for a Dbspace* on page 1151
- *Generating Dbspace DDL Commands* on page 1152
- *Changing a Dbspace to Read-Only* on page 1153

- *Viewing or Modifying Dbspace Properties* on page 1154
- *Granting Dbspace CREATE Permission* on page 1157
- *Revoking Dbspace CREATE Permission* on page 1158
- *Dbspace Privilege Summary* on page 1159
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting (Dropping) a Dbspace

Delete (drop) a dbspace from the database.

Prerequisites

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- For catalog dbspaces, you are the only user connected to the database.
- The dbspace being dropped contains no user data or user-created objects.
- For a dbspace in an RLV store, there are no existing RLV-enabled tables, and the RLV dbspace is read-only.

Note: Dropping the dbspace from the RLV store prevents the creation of new RLV-enabled tables.

Task

You may drop dbspaces from the IQ main store or system store (catalog store), as long as at least one dbspace in read-write mode remains. You cannot drop the six initial dbspaces (SYSTEM, TEMPORARY, IQ_SHARED_TEMP, IQ_SYSTEM_MAIN, IQ_SYSTEM_TEMP, and IQ_SYSTEM_MSG).

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Space Management > Dbspaces**.
3. Select one or more dbspaces from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple dbspaces.

- Click **Yes** to confirm deletion.

See also

- *Creating a Dbspace* on page 1148
- *Preallocating Space for a Dbspace* on page 1151
- *Generating Dbspace DDL Commands* on page 1152
- *Changing a Dbspace to Read-Only* on page 1153
- *Viewing or Modifying Dbspace Properties* on page 1154
- *Granting Dbspace CREATE Permission* on page 1157
- *Revoking Dbspace CREATE Permission* on page 1158
- *Dbspace Privilege Summary* on page 1159
- *Authenticating a Login Account for a Managed Resource* on page 282

Preallocating Space for a Dbspace

Preallocate space for a catalog dbspace.

Prerequisites

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

This operation is valid only for catalog dbspaces. You cannot preallocate space for a dbspace in the IQ Main or RLV stores.

Sybase IQ automatically increases the size of catalog DB files as additional space is needed. If your database has a high rate of change, you can preallocate disk space for dbspaces. Proper preallocation reduces fragmentation and improves performance.

- In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
- In the left pane, select **IQ Servers > Space Management > Dbspaces**.
- Select a dbspace from the right pane and either:
 - Click the arrow to the right of the name and select **Pre-allocate Space**, or

- From the Administration Console menu bar, select **Resource > Pre-allocate Space**.
4. Specify space to preallocate and the unit of measure, for example, **2 megabytes**.
 5. Click **OK**.

See also

- *Creating a Dbspace* on page 1148
- *Deleting (Dropping) a Dbspace* on page 1150
- *Generating Dbspace DDL Commands* on page 1152
- *Changing a Dbspace to Read-Only* on page 1153
- *Viewing or Modifying Dbspace Properties* on page 1154
- *Granting Dbspace CREATE Permission* on page 1157
- *Revoking Dbspace CREATE Permission* on page 1158
- *Dbspace Privilege Summary* on page 1159
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Dbspace DDL Commands

Display the data description language SQL code for creating a dbspace. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Space Management > Dbspaces**.
3. Select one or more dbspaces from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple dbspaces.

The DDL view shows the SQL code used to create the selected dbspaces.

See also

- *Creating a Dbspace* on page 1148
- *Deleting (Dropping) a Dbspace* on page 1150
- *Preallocating Space for a Dbspace* on page 1151
- *Changing a Dbspace to Read-Only* on page 1153
- *Viewing or Modifying Dbspace Properties* on page 1154
- *Granting Dbspace CREATE Permission* on page 1157
- *Revoking Dbspace CREATE Permission* on page 1158
- *Dbspace Privilege Summary* on page 1159
- *Authenticating a Login Account for a Managed Resource* on page 282

Changing a Dbspace to Read-Only

Change a dbspace to read-only mode.

Prerequisites

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

You can add a new DB file to a read-only dbspace. You cannot delete a DB file from a read-only dbspace.

You can change paths of DB files in a read-only offline dbspace.

Note: Changing the file path here does not move the file to the new location. If a file is moved, changing the path here only informs the SAP Sybase IQ server of the new file location.

IQ_SYSTEM_MAIN and IQ_SHARED_TEMP dbspaces cannot be read-only.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Space Management > Dbspaces**.
3. Select a dbspace from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or

- From the Administration Console menu bar, select **Resource > Properties**.

The Dbspace Properties view appears.

4. On the General page, click **ReadOnly** mode.
5. Set Status to **Online** or **Offline**.
6. Click **OK**.

See also

- *Creating a Dbspace* on page 1148
- *Deleting (Dropping) a Dbspace* on page 1150
- *Preallocating Space for a Dbspace* on page 1151
- *Generating Dbspace DDL Commands* on page 1152
- *Viewing or Modifying Dbspace Properties* on page 1154
- *Granting Dbspace CREATE Permission* on page 1157
- *Revoking Dbspace CREATE Permission* on page 1158
- *Dbspace Privilege Summary* on page 1159
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Dbspace Properties

View or change the name, mode, status, and striping properties of a dbspace.

Prerequisites

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any dbspace property page – None required.</p> <p>Modify dbspace permissions – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority. <p>Modify any other dbspace property – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• SPACE ADMIN authority.
SAP Sybase IQ 16.0	<p>View any dbspace property page – None required.</p> <p>Modify dbspace permissions – Requires MANAGE ANY DBSPACE system privilege.</p> <p>Modify any other dbspace property – Requires MANAGE ANY DBSPACE system privilege.</p>

- The SAP Sybase IQ resource is authenticated and running.

Task

You cannot change a dbspace's name if it is a system dbspace (with a name beginning with IQ_SYSTEM) or a system catalog dbspace.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Space Management > Dbspaces**.
3. Select a dbspace from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Dbspace Properties view appears.

4. View or modify the properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.
 - Some properties are read-only or hidden, based on the dbspace type.

Area	Description
General	<p>Name – Name of the dbspace.</p> <p>Type – (Read-only) The dbspace type.</p> <p>Mode – Mode of the dbspace. Available values are:</p> <ul style="list-style-type: none"> • ReadWrite • ReadOnly <p>Status – Status of the dbspace. Available values are:</p> <ul style="list-style-type: none"> • Online • Offline <p>Striping – Enables (On) or disables (Off) disk striping for this dbspace.</p> <p>Stripe size – The number of kilobytes (KB) to write to each file before the disk-striping algorithm moves to the next stripe for this dbspace.</p> <p>File – (for Catalog type only)</p> <p>Reallocate Space – (for Catalog type only)</p> <hr/> <p>Note:</p> <ul style="list-style-type: none"> • The RLV store dbspace can be renamed if no RLV-enabled tables exist. • The mode of the RLV store dbspace can be changed, if the dbspace is online, however ReadOnly mode can only be selected if no RLV-enabled tables exist. • The status of the RLV store dbspace can be changed, if the dbspace is in ReadOnly mode. • Striping and Stripe Size are not supported for the RLV store dbspace.
DB Files	To manage the db files within the dbspace, click the arrow to the right of a db file name and select an option.
Permissions	See <i>Granting Dbspace CREATE Permission</i> on page 1157 and <i>Revoking Dbspace CREASTE Permission</i> on page 1158.

5. Click **OK**.

See also

- *Creating a Dbspace* on page 1148
- *Deleting (Dropping) a Dbspace* on page 1150
- *Preallocating Space for a Dbspace* on page 1151
- *Generating Dbspace DDL Commands* on page 1152

- *Changing a Dbspace to Read-Only* on page 1153
- *Granting Dbspace CREATE Permission* on page 1157
- *Revoking Dbspace CREATE Permission* on page 1158
- *Dbspace Privilege Summary* on page 1159
- *Authenticating a Login Account for a Managed Resource* on page 282

Granting Dbspace CREATE Permission

Grant dbspace create permission to users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Space Management > Dbspaces**.
3. Select a dbspace from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Dbspace Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
6. On the Welcome page, indicate whether the permission is being granted to a user or role.
7. Click **Next**.
8. On the Grantees page, select one or more users or roles. Click the box in the header row to select all available users or roles.
9. Click **Next**.

10. On the Permissions page, ensure **Create** is selected.

11. Click **Finish**.

12. Click **OK**.

See also

- *Creating a Dbspace* on page 1148
- *Deleting (Dropping) a Dbspace* on page 1150
- *Preallocating Space for a Dbspace* on page 1151
- *Generating Dbspace DDL Commands* on page 1152
- *Changing a Dbspace to Read-Only* on page 1153
- *Viewing or Modifying Dbspace Properties* on page 1154
- *Revoking Dbspace CREATE Permission* on page 1158
- *Dbspace Privilege Summary* on page 1159
- *Authenticating a Login Account for a Managed Resource* on page 282

Revoking Dbspace CREATE Permission

Remove dbspace create permission from users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Space Management > Dbspaces**.
3. Select a dbspace from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Dbspace Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, select a grantee, and click **Revoke**.
6. Click **OK**.

See also

- *Creating a Dbspace* on page 1148
- *Deleting (Dropping) a Dbspace* on page 1150
- *Preallocating Space for a Dbspace* on page 1151
- *Generating Dbspace DDL Commands* on page 1152
- *Changing a Dbspace to Read-Only* on page 1153
- *Viewing or Modifying Dbspace Properties* on page 1154
- *Granting Dbspace CREATE Permission* on page 1157
- *Dbspace Privilege Summary* on page 1159
- *Authenticating a Login Account for a Managed Resource* on page 282

Dbspace Privilege Summary

A list of the system privileges and object permissions required to complete the various dbspace tasks.

Creating a Dbspace

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Deleting a Dbspace

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Preallocating Space for a Dbspace

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Generating Dbspace DDL Commands

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Changing a Dbspace to Read-Only

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Viewing or Modifying Dbspace Properties

Database Version	Dbspace Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any dbspace property page – None required.</p> <p>Modify dbspace permissions – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. <p>Modify any other dbspace property – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.

Database Version	DbSPACE Privileges
SAP Sybase IQ 16.0	<p>View any dbSPACE property page – None required.</p> <p>Modify dbSPACE permissions – Requires MANAGE ANY DBSPACE system privilege.</p> <p>Modify any other dbSPACE property – Requires MANAGE ANY DBSPACE system privilege.</p>

Granting and Revoking DbSPACE CREATE Permission

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

See also

- *Creating a DbSPACE* on page 1148
- *Deleting (Dropping) a DbSPACE* on page 1150
- *Preallocating Space for a DbSPACE* on page 1151
- *Generating DbSPACE DDL Commands* on page 1152
- *Changing a DbSPACE to Read-Only* on page 1153
- *Viewing or Modifying DbSPACE Properties* on page 1154
- *Granting DbSPACE CREATE Permission* on page 1157
- *Revoking DbSPACE CREATE Permission* on page 1158

DB Files

Add, modify, view properties, or delete a database file.

Creating a DB File

Add a DB file to a dbspace.

Prerequisites

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

Follow these steps to add files to all shared dbspaces: IQ_SYSTEM_MAIN, IQ_SHARED_TEMP, and all user-defined dbspaces.

Note: Adding DB files to IQ_SYSTEM_MAIN synchronizes all running secondary nodes.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Space Management > DB Files**.
3. Click the arrow next to **DB Files** and select **New**.
The Create DB File wizard appears.
4. On the DB Files page, select the resource and the dbspace to which you are adding the DB file.
5. Click **Add**.

Note: DB files can only be added to the RLV store dbspace when it is online. The RLV dbspace can either be in ReadOnly or ReadWrite mode, however files can only be added in ReadWrite mode when there are no RLV-enabled objects.

6. On the DB File Details page, specify:

Option	Description
Logical name	User-defined name of the DB file.

Option	Description
Path to physical file on disk	Path to the physical file on disk. It is usually best to use an absolute path. A relative path works for simplex servers and for multiplexes that use the SCC shared-disk facility and have the SCC installation directory mounted in the same location on each multiplex server host. If you specify a relative path for a simplex that is later converted to a multiplex, the relative path might cause an error.
Raw device	A check mark indicates the file is on a raw device.
File size	Space you allocate to the DB file in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB). Unavailable on raw devices; required if the file is not on a raw device. Minimum file size is 8 MB.
Reserve size	(Optional; default is 0.) Extra space you allocate to the DB File in kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB). You can use this space to increase the file size if the file grows. Guideline: reserve size should be about 30% of file size.
Mode	(Optional) <ul style="list-style-type: none"> • Read Only • Read/Write • Force Read/Write <hr/> Note: This option appears only if you are adding DB files to the <code>IQ_SHARED_TEMP</code> dbspace in a multiplex setup.

7. Click **Finish**.

Next

Create a Dbspace File Size in Use alert to warn you if the DB file exceeds a set percentage of the configured file size (70%, for example). If the alert is activated, you can increase the file size. To enable this alert, first schedule a data collection that includes its key performance indicator, such as the Dbspace File Statistics Collection or All Stats w/o Availability.

See also

- *Deleting a DB File* on page 1164
- *Emptying a DB File* on page 1165
- *Generating DB File DDL Commands* on page 1166
- *Viewing or Modifying DB File Properties* on page 1167
- *DB File Privilege Summary* on page 1169
- *SAP Sybase IQ Data Collections* on page 286
- *Authenticating a Login Account for a Managed Resource* on page 282

- *Creating an Alert* on page 295

Deleting a DB File

Delete a DB file from a dbspace. With the exception of the IQ_SHARED_TEMP dbspace, you cannot delete the last DB file in a dbspace.

Prerequisites

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The dbspace must be in read-write mode, except for the RLV store dbspace, which can be in either mode.
- The DB file must be empty.
- The last DB file in a dbspace cannot be deleted, except for IQ_SHARED_TEMP. In IQ_SHARED_TEMP, the last DB file can only be deleted on the coordinator once it is started in a single-node mode. Dropping files in IQ_SHARED_TEMP in simplex is also supported. The first file that is made Read-Write in IQ_SHARED_TEMP must be the last file dropped.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Space Management > DB Files**.
3. Select one or more DB files from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple dbfiles.

4. Click **Yes** to confirm deletion.

See also

- *Creating a DB File* on page 1162
- *Emptying a DB File* on page 1165
- *Generating DB File DDL Commands* on page 1166

- *Viewing or Modifying DB File Properties* on page 1167
- *DB File Privilege Summary* on page 1169
- *Authenticating a Login Account for a Managed Resource* on page 282

Emptying a DB File

Empty a DB file and move the objects in the file to another available read-write DB file.

Prerequisites

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- The dbspace must be in read-write mode.
- The DB file should be read-only.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Space Management > Db Files**.
3. Select a db file from the right pane and either:
 - Click the arrow to the right of the name and select **Empty File**, or
 - From the Administration Console menu bar, select **Resource > Empty File**.

Note: You cannot empty a db file belonging to the RLV store dbspace.

4. Click **Yes**.
Objects in the DB file are moved to another read-write DB file in the same dbspace.

See also

- *Creating a DB File* on page 1162
- *Deleting a DB File* on page 1164
- *Generating DB File DDL Commands* on page 1166
- *Viewing or Modifying DB File Properties* on page 1167
- *DB File Privilege Summary* on page 1169
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating DB File DDL Commands

Display the data description language SQL code for adding a DB file to a dbspace. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Space Management > Db Files**.
3. Select one or more db files from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple db files.

The DDL view shows the SQL code used to create the selected db files.

See also

- *Creating a DB File* on page 1162
- *Deleting a DB File* on page 1164
- *Emptying a DB File* on page 1165
- *Viewing or Modifying DB File Properties* on page 1167
- *DB File Privilege Summary* on page 1169
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying DB File Properties

Display and change the name, mode, and path properties of a DB file.

Prerequisites

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	View any db file property page – None required. Modify any db file property – Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	View any db file property page – None required. Modify any db file property – Requires MANAGE ANY DBSPACE system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

The mode and status of the DB file determine which properties can be modified.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Space Management > Db Files**.
3. Select a db file from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Db File Properties view appears.

4. View or modify the properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.
 - The mode and status of the DB file determine which properties can be modified.

Property	Description
Name	Logical file name. If the dbspace is in Read Only mode and OFFLINE status, you cannot change the name of the DB file.

Property	Description
Path (Read-only)	<p>Location of the physical file or raw partition. You can modify the path only when the dbspace's status is OFFLINE. You cannot change the path for DB files in the RLV store dbspace.</p> <p>It is usually best to use an absolute path. A relative path works for simplex servers and for multiplexes that use the SCC shared-disk facility and have the SCC installation directory mounted in the same location on each multiplex server host. If you specify a relative path for a simplex that is later converted to a multiplex, the relative path might cause an error.</p>
Mode	<p>Mode of the dbspace:</p> <ul style="list-style-type: none"> • Read Only • Read/Write • Force Read/Write <p>You cannot change the mode for DB files in the RLV store dbspace.</p>
File size (Read-only)	Current size of the file or raw partition. Use the Modify file size field to change the file size.
Reserved size (Read-only)	Reserved space in the dbspace that you can add to this DB file. Use the Modify file size field to transfer space between the reserved size and the file size.
Total size (Read-only)	Current size of the file plus the size of the reserved space.
Modify file size	<p>Enter a new value for file size.</p> <p>You cannot increase the file size by more than the reserved size. For example, if the file size is 100 MB and the reserve is 30 MB, the maximum permissible file size is 130 MB.</p> <p>You can only change the file size for DB files in the RLV store dbspace when the dbspace is in Read/Write mode. You can only reduce the file size if the truncated space is not in use.</p>
Dbspace (Read-only)	Name of the dbspace.
Status (Read-only)	<p>Status of the dbspace:</p> <ul style="list-style-type: none"> • ONLINE • OFFLINE

5. Click **OK**.

See also

- *Creating a DB File* on page 1162
- *Deleting a DB File* on page 1164
- *Emptying a DB File* on page 1165
- *Generating DB File DDL Commands* on page 1166
- *DB File Privilege Summary* on page 1169
- *Authenticating a Login Account for a Managed Resource* on page 282

DB File Privilege Summary

A list of the system privileges and object permissions required to complete the various DB file tasks.

Creating a DB File

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Deleting a DB File

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Emptying a DB File

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.

Database Version	DB File Privileges
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

Generating DB File DDL Commands

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying DB File Properties

Database Version	DB File Privileges
SAP Sybase IQ 15.3 and 15.4	View any db file property page – None required. Modify any db file property – Requires one of: <ul style="list-style-type: none"> • DBA authority. • SPACE ADMIN authority.
SAP Sybase IQ 16.0	View any db file property page – None required. Modify any db file property – Requires MANAGE ANY DBSPACE system privilege.

Granting or Revoking Dbspace CREATE Permission

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY DBSPACE system privilege.

See also

- *Creating a DB File* on page 1162
- *Deleting a DB File* on page 1164
- *Emptying a DB File* on page 1165
- *Generating DB File DDL Commands* on page 1166
- *Viewing or Modifying DB File Properties* on page 1167

Events

You can automate routine tasks by adding an event to a database, and providing a schedule or conditional trigger for the event. In a multiplex, an event is a global object that is shared across all nodes participating in the multiplex.

There are three types of events:

- Scheduled events have an associated schedule and execute at specified times.
- Conditional events are associated with a system event, and an optional list of conditions that is tracked by the database server.
- Manual events can only be fired explicitly.

After each execution of an event handler, a COMMIT occurs if no errors occurred. A ROLLBACK occurs if there was an error.

Creating an Event

Create a new event, set to be triggered manually, by a schedule or by a system event and specific conditions.

Prerequisites

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY EVENT system privilege. • CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Click the arrow next to **Events** and select **New**.
The Create Event wizard appears.
4. On the Welcome page, specify:

Option	Description
Resource	The resource on which the event will be created.
Name of event to create	A name for the event, unique for this user.
User	The user who will own the event.

5. Click **Next**.
6. On the Event Trigger page, specify the circumstance or condition that will trigger the event:

Option	Description
Manual Event	The event will be triggered explicitly when you use the TRIGGER EVENT statement or select the Trigger menu option.
Scheduled Event	You will be able to create a schedule so that the event will execute at specified times.
Conditional Event	You will be able to specify a system event and optional trigger conditions that will trigger the event.

7. Click **Next**.
8. (Scheduled Events only) On the Schedule page, specify the details of the initial schedule. (You can create additional schedules later, through the Schedule Properties wizard).

Option	Description
Schedule Name	A name for the schedule, unique for this user.
Time	The time, or start and end time duration, in 24 h format, when the event will run (either once or the interval you specify on the Recurrence Page).
Date	(Optional) The date on which the event will first run.

9. Click **Next**.
10. (Scheduled Events only) On the Recurrence page, specify how often to trigger the event and the days to run the event:

Option	Description
Trigger Repeatedly	The recurrence interval for the event
Specific Days	The days of the week or month when the event will be triggered.

11. Click **Next**.

12. (Conditional Events only) On the Conditions page, specify condition details:

Option	Description
System Event	Select the system event which will trigger the event
Trigger Conditions	(Optional) Set one or more trigger conditions that must be satisfied, in addition to the system event, in order to trigger the event. Use the New , Edit and Delete buttons to manage the trigger conditions.

13. Click **Next**.

14. On the Options page, complete additional details for the event:

Option	Description
Enable Event	Select the checkbox to execute the event when the scheduled time, trigger condition or manual command occurs. If unchecked, the event is created, but will not run until you later enable it.
Location	Specify where the event will run: <ul style="list-style-type: none"> • Execute at all databases — Executes the event at any and all remote locations. • Execute at the consolidated databases only — For databases involved in SQL Remote replication, this executes the event at the consolidated database only, and not at any of the remote locations. • Execute at the remote databases only — For databases involved in SQL Remote replication, this executes the event at the remote database(s) only, and not at the consolidated database.

15. Click **Next**.

16. (Optional) On the Comment page, enter a comment about the event.

17. Click **Finish**.

See also

- *Deleting an Event* on page 1174
- *Disabling an Event* on page 1175
- *Enabling an Event* on page 1176
- *Triggering an Event* on page 1177
- *Generating Event DDL Commands* on page 1178
- *Viewing or Modifying Event Properties* on page 1179
- *Event Schedules* on page 1181
- *Event Privilege Summary* on page 1186
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting an Event

Permanently delete an event and all associated event schedules and triggers.

Prerequisites

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. DROP ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Select one or more events from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple events.

4. Click **Yes** to confirm deletion.

See also

- *Creating an Event* on page 1171
- *Disabling an Event* on page 1175
- *Enabling an Event* on page 1176
- *Triggering an Event* on page 1177
- *Generating Event DDL Commands* on page 1178
- *Viewing or Modifying Event Properties* on page 1179
- *Event Schedules* on page 1181
- *Event Privilege Summary* on page 1186
- *Authenticating a Login Account for a Managed Resource* on page 282

Disabling an Event

Disable a currently enabled event.

Prerequisites

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. ALTER ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- An event has been created, and enabled.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Select one or more events from the right pane, click the arrow to the right of the name and select **Disable**.

Tip: Use **Shift-click** or **Control-click** to select multiple events.

4. Click **Yes** to confirm disable.

See also

- *Creating an Event* on page 1171
- *Deleting an Event* on page 1174
- *Enabling an Event* on page 1176
- *Triggering an Event* on page 1177
- *Generating Event DDL Commands* on page 1178
- *Viewing or Modifying Event Properties* on page 1179
- *Event Schedules* on page 1181
- *Event Privilege Summary* on page 1186
- *Authenticating a Login Account for a Managed Resource* on page 282

Enabling an Event

Enable a currently disabled event.

Prerequisites

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. ALTER ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- An event has been created, and disabled.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Select one or more events from the right pane, click the arrow to the right of the name and select **Enable**.

Tip: Use **Shift-click** or **Control-click** to select multiple events.

4. Click **Yes** to confirm enable.

See also

- *Creating an Event* on page 1171
- *Deleting an Event* on page 1174
- *Disabling an Event* on page 1175
- *Triggering an Event* on page 1177
- *Generating Event DDL Commands* on page 1178
- *Viewing or Modifying Event Properties* on page 1179
- *Event Schedules* on page 1181
- *Event Privilege Summary* on page 1186
- *Authenticating a Login Account for a Managed Resource* on page 282

Triggering an Event

Execute an event. You can trigger an event manually regardless of its type (manual, scheduled, or conditional). The TRIGGER EVENT statement can be called at any time for any event.

Prerequisites

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EVENT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- An event has been created.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Select an event from the right pane, click the arrow to the right of the name and select **Trigger**.
4. (Optional) Enter event parameters.

This dialog allows you to explicitly supply parameters to simulate a context for the event handler. You can use this dialog to test trigger conditions such as disk space restrictions (when a disk fills beyond a specified percentage) or other trigger conditions that are required to trigger an event handler. For example, you can have an event that takes different actions depending which user ID is connected to the database: calling the event parameter ('User') in the event handler does this. To simulate triggering this event for the user P_Chin, type the following in the Parameters text box: "User"='P_Chin' The word User must be contained in double quotes because it is a reserved word in SQL.

5. Click **OK** to confirm trigger.

See also

- *Creating an Event* on page 1171
- *Deleting an Event* on page 1174
- *Disabling an Event* on page 1175
- *Enabling an Event* on page 1176
- *Generating Event DDL Commands* on page 1178
- *Viewing or Modifying Event Properties* on page 1179
- *Event Schedules* on page 1181

- *Event Privilege Summary* on page 1186
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Event DDL Commands

Display the SQL data description language for creating a new event. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Select the event from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**

The DDL view opens, showing the SQL code used to create the selected event.

See also

- *Creating an Event* on page 1171
- *Deleting an Event* on page 1174
- *Disabling an Event* on page 1175
- *Enabling an Event* on page 1176
- *Triggering an Event* on page 1177
- *Viewing or Modifying Event Properties* on page 1179
- *Event Schedules* on page 1181
- *Event Privilege Summary* on page 1186
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Event Properties

Display or change the properties of the selected event.

Prerequisites

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	View event properties – None required. Modify event comment or properties – Requires DBA authority.
SAP Sybase IQ 16.0	View event properties only – None required. Modify event properties – Requires one of: <ul style="list-style-type: none"> • MANAGE ANY EVENT system privilege. • ALTER ANY OBJECT system privilege. Modify event comment only – Requires one of: <ul style="list-style-type: none"> • MANAGE ANY EVENT system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Select an events from the right pane, click the arrow to the right of the name and select **Properties**.
The Event Properties view appears.
4. View or modify the properties.

Area	Description
General	<p>Name – (Read-only) Name of the event.</p> <p>Owner – (Read-only) Name of the owner of the event.</p> <p>Running – (Read-only) Indicates whether the event is running.</p> <p>Enabled – Select the check box to execute the event when the scheduled time, trigger condition or manual command occurs.</p> <p>Location – (Read-only) Indicates where the event will run. Valid values are:</p> <ul style="list-style-type: none"> • Execute at all databases – Executes the event at any and all remote locations. • Execute at the consolidated databases only –For databases involved in SQL Remote replication, this executes the event at the consolidated database only, and not at any of the remote locations. • Execute at the remote databases only – For databases involved in SQL Remote replication, this executes the event at the remote database(s) only, and not at the consolidated database. <p>Next scheduled time – (Read-only) The time next time the event is scheduled to run.</p> <p>Comment – Add an optional comment about the event.</p>
SQL	Displays the SQL statements that are executed when the event is triggered. If you edit the SQL code, click Apply before leaving the page.
Schedules	Use the New , Edit and Delete buttons to manage the event's schedules.
Conditions	<p>System Event – From the drop down list, view or change the system event which triggers the event.</p> <p>Conditions – (Optional) Set one or more trigger conditions that must be satisfied, in addition to the system event, in order to trigger the event. Use the New, Edit and Delete buttons to manage the trigger conditions.</p>

5. Click **OK** to save any changes, and exit the Event Properties view.

See also

- *Creating an Event* on page 1171
- *Deleting an Event* on page 1174
- *Disabling an Event* on page 1175
- *Enabling an Event* on page 1176
- *Triggering an Event* on page 1177
- *Generating Event DDL Commands* on page 1178

- *Event Schedules* on page 1181
- *Event Privilege Summary* on page 1186
- *Authenticating a Login Account for a Managed Resource* on page 282

Event Schedules

You can schedule an event to run at a specific date, time or duration, once or at a recurring interval. An event can have more than one schedule.

See also

- *Creating an Event* on page 1171
- *Deleting an Event* on page 1174
- *Disabling an Event* on page 1175
- *Enabling an Event* on page 1176
- *Triggering an Event* on page 1177
- *Generating Event DDL Commands* on page 1178
- *Viewing or Modifying Event Properties* on page 1179
- *Event Privilege Summary* on page 1186

Creating an Event Schedule

Make a new schedule for an existing event.

Prerequisites

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • <code>MANAGE ANY EVENT</code> system privilege. • <code>ALTER ANY OBJECT</code> system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Select an event from the right pane, click the arrow to the right of the name and select **Properties**.

The Event Properties view appears.

4. Select the **Schedules** page.
5. Select **New**.
The Create Schedule Wizard appears.
6. On the Schedule page, specify the details of the schedule.

Option	Description
Schedule Name	A unique name for the schedule
Time	The time or start and end times, in 24 h format, when the event will run.
Date	(Optional) The date on which the event will run.

7. Click **Next**.
8. On the Recurrence page, specify how often to trigger the event and the days to run the event:

Option	Description
Trigger Repeatedly	The recurrence interval for the event
Specific Days	The days of the week or month when the event will run.

9. Click **Finish** to save changes, and exit the Create Schedule wizard.
10. Click **OK** to exit the Schedules page, and the Event Properties view.

See also

- *Deleting an Event Schedule* on page 1182
- *Generating Event Schedule DDL Commands* on page 1183
- *Modifying Event Schedule Properties* on page 1184
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting an Event Schedule

Delete one or more schedule(s) for a selected event.

Prerequisites

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.

Database Version	Event Schedule Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. ALTER ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Select an event from the right pane, click the arrow to the right of the name and select **Properties**.
The Event Properties view appears.
4. Select the **Schedules** page.
5. Select one or more previously created schedule for the event, and select **Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple schedules.

6. Click **OK** to delete selected schedules and exit the Schedules page and the Event Properties view.

See also

- *Creating an Event Schedule* on page 1181
- *Generating Event Schedule DDL Commands* on page 1183
- *Modifying Event Schedule Properties* on page 1184
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Event Schedule DDL Commands

Display the SQL data description language for creating a new schedule for a selected event. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Select an event from the right pane, click the arrow to the right of the name and select **Properties**.
The Event Properties view appears.
4. Select the **Schedules** area.
5. Select a previously created schedule for the event, and select **Generate DDL**.
The DDL view opens, showing the SQL code used to create the selected event schedule.

See also

- *Creating an Event Schedule* on page 1181
- *Deleting an Event Schedule* on page 1182
- *Modifying Event Schedule Properties* on page 1184
- *Authenticating a Login Account for a Managed Resource* on page 282

Modifying Event Schedule Properties

Edit the properties of a schedule for a selected event.

Prerequisites

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	View any event schedule property page – None required. Modify any event schedule property – Requires DBA authority.
SAP Sybase IQ 16.0	View any event schedule property page – None required. Modify any event schedule property – Requires one of: <ul style="list-style-type: none">• <code>MANAGE ANY EVENT</code> system privilege.• <code>ALTER ANY OBJECT</code> system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Events**.
3. Select an event from the right pane, click the arrow to the right of the name and select **Properties**.
The Event Properties view appears.
4. Select the **Schedules** page.
5. Select a previously created schedule for the event, and select **Edit**.
The Schedule Properties view appears.
6. View or modify the properties.

Area	Description
General	Displays the values specified when the schedule was created. Editable fields are: Start Time – The time, or start and end times, in 24 h format, when the event will run. Start Date – (Optional) The date on which the event will run.
Recurrence	Trigger Repeatedly – The recurrence interval for the event. Specific Days – The days of the week or month when the event will run.

7. Click **OK** to save changes, and exit the Schedule Properties view.
8. Click **OK** to exit the Schedules page, and the Event Properties view.

See also

- *Creating an Event Schedule* on page 1181
- *Deleting an Event Schedule* on page 1182
- *Generating Event Schedule DDL Commands* on page 1183
- *Authenticating a Login Account for a Managed Resource* on page 282

Event Privilege Summary

A list of the system privileges and object permissions required to complete the various event tasks.

Creating an Event

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • <code>MANAGE ANY EVENT</code> system privilege. • <code>CREATE ANY OBJECT</code> system privilege.

Deleting an Event

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • <code>MANAGE ANY EVENT</code> system privilege. • <code>DROP ANY OBJECT</code> system privilege.

Disabling or Enabling an Event

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • <code>MANAGE ANY EVENT</code> system privilege. • <code>ALTER ANY OBJECT</code> system privilege.

Triggering an Event

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.

Database Version	Event Privileges
SAP Sybase IQ 16.0	Requires MANAGE ANY EVENT system privilege.

Generating Event DDL Commands

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Event Properties

Database Version	Event Privileges
SAP Sybase IQ 15.3 and 15.4	View event properties – None required. Modify event comment or properties – Requires DBA authority.
SAP Sybase IQ 16.0	View event properties only – None required. Modify event properties – Requires one of: <ul style="list-style-type: none"> • MANAGE ANY EVENT system privilege. • ALTER ANY OBJECT system privilege. Modify event comment only – Requires one of: <ul style="list-style-type: none"> • MANAGE ANY EVENT system privilege • CREATE ANY OBJECT system privilege • ALTER ANY OBJECT system privilege • COMMENT ANY OBJECT system privilege

Creating an Event Schedule

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY EVENT system privilege. • ALTER ANY OBJECT system privilege.

Deleting an Event Schedule

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. ALTER ANY OBJECT system privilege.

Generating Event Schedule DDL Commands

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

*Viewing or Modifying Event Schedule**Properties*

Database Version	Event Schedule Privileges
SAP Sybase IQ 15.3 and 15.4	View any event schedule property page – None required. Modify any event schedule property – Requires DBA authority.
SAP Sybase IQ 16.0	View any event schedule property page – None required. Modify any event schedule property – Requires one of: <ul style="list-style-type: none"> MANAGE ANY EVENT system privilege. ALTER ANY OBJECT system privilege.

See also

- *Creating an Event* on page 1171
- *Deleting an Event* on page 1174
- *Disabling an Event* on page 1175
- *Enabling an Event* on page 1176
- *Triggering an Event* on page 1177
- *Generating Event DDL Commands* on page 1178
- *Viewing or Modifying Event Properties* on page 1179
- *Event Schedules* on page 1181

External Environments

Install, delete, update, and modify the components of external development environments.

Working in a Java External Environment

Install and manage Java classes and JAR files. Test a Java external environment and modify its properties.

See also

- *Working in a Perl External Environment* on page 1204
- *Working in a PHP External Environment* on page 1215
- *Working in a C ESQL External Environment* on page 1226
- *Working in a C ODBC External Environment* on page 1228
- *Working in a CLR (.NET) External Environment* on page 1230

Installing a Java Classes File into an SAP Sybase IQ Database

Install a Java classes file to an SAP Sybase IQ database using Sybase Control Center. This enables the database to execute functions and procedures written in Java.

Prerequisites

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- Copy the Java classes file to a location accessible to the SAP Sybase IQ server.

Task

A Java external environment appears in the list of external environments in the Sybase Control Center Administration Console even when none of its classes files have been installed.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments > Java > Classes**.
3. Click the arrow beside Classes and select **New**.

The Install Java Classes wizard appears.

4. On the Welcome page, specify:

Option	Description
Select a Sybase IQ resource on which the Java class will be installed:	Select an SAP Sybase IQ resource from the list.
(Multiplex only) Select a multiplex server on which the Java class will be installed	Select a multiplex server from the list.
SCC agent status	Indicates the current status of the SCC agent. If the SCC agent is not registered, click Register Agent and enter the required registration information. If the SCC agent is not authenticated, click Authenticate Agent . Enter a user ID, password, and port for SCC to use when it logs in to the SCC agent.
Java class file path	Enter the path to the Java class file. It must be on a file system accessible to the SAP Sybase IQ resource.
Comment	(Optional) Enter a comment describing the class.

5. Click **Finish** to install the class.

See also

- *Updating a Java Classes File* on page 1191
- *Deleting a Classes File* on page 1192
- *Viewing or Modifying Java Classes File Properties* on page 1193
- *Installing a Java JAR File into an SAP Sybase IQ Database* on page 1194
- *Updating a Java JAR File* on page 1196
- *Deleting a JAR File* on page 1197
- *Viewing or Modifying the Java JAR File Properties* on page 1198
- *Testing the Configuration of a Java External Environment* on page 1200
- *Viewing or Modifying Java External Environment Properties* on page 1201
- *Java External Environment Privilege Summary* on page 1202
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Registering and Authenticating a Sybase Control Center Agent* on page 279

Updating a Java Classes File

Update a Java classes file in an SAP Sybase IQ database.

Prerequisites

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- Put an updated version of the Java classes file in a location accessible to the Sybase IQ server.

Task

- In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
- In the left pane, select **IQ Servers > Compiled Objects > External Environments > Java > Classes**.
- Select a class from the right pane and either:
 - Click the arrow to the right of the name and select **Update**, or
 - From the Administration Console menu bar, select **Properties > Update**.

The Update External Environment Object view appears.

- On the Update Java Clss page, if the **Register Agent** button is active, click it to register the SCC agent on the classes' Sybase IQ server. Enter the required registration information.
- If the **Authenticate Agent** button is active, click it to authenticate the SCC agent. Enter a user ID and password for SCC to use when it logs in to the SCC agent.
- Enter the path to the updated classes file. It must be on a file system accessible to the Sybase IQ resource.
- Click **Finish** to update the classes or JAR.

See also

- Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- Deleting a Classes File* on page 1192
- Viewing or Modifying Java Classes File Properties* on page 1193
- Installing a Java JAR File into an SAP Sybase IQ Database* on page 1194
- Updating a Java JAR File* on page 1196
- Deleting a JAR File* on page 1197
- Viewing or Modifying the Java JAR File Properties* on page 1198

- *Testing the Configuration of a Java External Environment* on page 1200
- *Viewing or Modifying Java External Environment Properties* on page 1201
- *Java External Environment Privilege Summary* on page 1202
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Registering and Authenticating a Sybase Control Center Agent* on page 279

Deleting a Classes File

Remove a standalone classes file from an SAP Sybase IQ database.

Prerequisites

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

You cannot remove classes that are part of a JAR. Use the Update feature to remove the classes from the JAR, then delete them.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments > Java > Classes**.
3. Select one or more classes files from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple classes files.

4. Review the confirmation dialog and click **Yes**.

See also

- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Updating a Java Classes File* on page 1191
- *Viewing or Modifying Java Classes File Properties* on page 1193
- *Installing a Java JAR File into an SAP Sybase IQ Database* on page 1194
- *Updating a Java JAR File* on page 1196
- *Deleting a JAR File* on page 1197

- *Viewing or Modifying the Java JAR File Properties* on page 1198
- *Testing the Configuration of a Java External Environment* on page 1200
- *Viewing or Modifying Java External Environment Properties* on page 1201
- *Java External Environment Privilege Summary* on page 1202
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Java Classes File Properties

Display the properties of a Java classes file associated with an SAP Sybase IQ database. Only the comment can be modified.

Prerequisites

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	View external environment properties – None required. Modify external environment properties – Requires DBA authority.
SAP Sybase IQ 16.0	View external environment properties – None required. Modify external environment properties – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments > Java > Classes**.
3. Select a class from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Java Class Properties view appears.

4. Edit the comments field if needed. All other properties are read-only.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) Name of the class.</p> <p>Type – (Read-only) Type of class.</p> <p>Creator – (Read-only) User who created the class.</p> <p>JAR – (Read-only) The name of the JAR containing the class file.</p> <p>Time created – (Read-only) Date and time the class file was created.</p> <p>Time modified – (Read-only) Date and time the class file was last modified.</p> <p>Comment – A text field for adding an optional comment about the class file.</p>

- Click **OK** to save any changes and closed the view.

See also

- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Updating a Java Classes File* on page 1191
- *Deleting a Classes File* on page 1192
- *Installing a Java JAR File into an SAP Sybase IQ Database* on page 1194
- *Updating a Java JAR File* on page 1196
- *Deleting a JAR File* on page 1197
- *Viewing or Modifying the Java JAR File Properties* on page 1198
- *Testing the Configuration of a Java External Environment* on page 1200
- *Viewing or Modifying Java External Environment Properties* on page 1201
- *Java External Environment Privilege Summary* on page 1202
- *Authenticating a Login Account for a Managed Resource* on page 282

Installing a Java JAR File into an SAP Sybase IQ Database

Install a Java JAR file to an SAP Sybase IQ database. This enables the database to execute functions and procedures written in Java.

Prerequisites

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- Copy the Java JAR file to a location accessible to the SAP Sybase IQ server.

Task

A Java external environment appears in the list of external environments in the Sybase Control Center Administration Console even when none of its JAR files have been installed.

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > External Environments > Java > JARs**.
3. Click the arrow beside JARs and select **New**.
The Install JARs wizard appears.
4. On the Welcome page, specify:

Option	Description
Select an SAP Sybase IQ resource on which the JAR file will be installed:	Select an SAP Sybase IQ resource from the list.
(Multiplex only) Select a multiplex server on which the JAR will be installed	Select a multiplex server from the list.
SCC agent status	Indicates the current status of the SCC agent. If the SCC agent is not registered, click Register Agent and enter the required registration information. If the SCC agent is not authenticated, click Authenticate Agent . Enter a user ID, password, and port for SCC to use when it logs in to the SCC agent.
JAR file path	Enter the path to the JAR file. It must be on a file system accessible to the SAP Sybase IQ resource
JAR name	Enter a unique name for the JAR file.
Comment	(Optional) Enter a comment describing the class or JAR.

5. Click **Next**.
6. On the Select Classes page, select all classes or a subset of the classes to install from the JAR.
7. Click **Finish** to install the class or JAR.

See also

- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Updating a Java Classes File* on page 1191
- *Deleting a Classes File* on page 1192

- *Viewing or Modifying Java Classes File Properties* on page 1193
- *Updating a Java JAR File* on page 1196
- *Deleting a JAR File* on page 1197
- *Viewing or Modifying the Java JAR File Properties* on page 1198
- *Testing the Configuration of a Java External Environment* on page 1200
- *Viewing or Modifying Java External Environment Properties* on page 1201
- *Java External Environment Privilege Summary* on page 1202
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Registering and Authenticating a Sybase Control Center Agent* on page 279

Updating a Java JAR File

Update a Java JAR file in an SAP Sybase IQ database.

Prerequisites

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- Put an updated version of the Java JAR file in a location accessible to the Sybase IQ server.

Task

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > External Environments > Java > JARs**.
3. Select a JAR file from the right pane and either:

- Click the arrow to the right of the name and select **Update**, or
- From the Administration Console menu bar, select **Properties > Update**.

The Update External Environment Object view appears.

4. On the Update Class page, if the **Register Agent** button is active, click it to register the SCC agent on the JAR's SAP Sybase IQ server. Enter the required registration information.
5. If the **Authenticate Agent** button is active, click it to authenticate the SCC agent. Enter a user ID and password for SCC to use when it logs in to the SCC agent.
6. Enter the path to the updated JAR file. It must be on a file system accessible to the SAP Sybase IQ resource.

7. Click **Next**.
8. Select the classes to update in the JAR.
9. Click **Finish**.

See also

- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Updating a Java Classes File* on page 1191
- *Deleting a Classes File* on page 1192
- *Viewing or Modifying Java Classes File Properties* on page 1193
- *Installing a Java JAR File into an SAP Sybase IQ Database* on page 1194
- *Deleting a JAR File* on page 1197
- *Viewing or Modifying the Java JAR File Properties* on page 1198
- *Testing the Configuration of a Java External Environment* on page 1200
- *Viewing or Modifying Java External Environment Properties* on page 1201
- *Java External Environment Privilege Summary* on page 1202
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Registering and Authenticating a Sybase Control Center Agent* on page 279

Deleting a JAR File

Remove a JAR file from an SAP Sybase IQ database.

Prerequisites

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

You cannot use this procedure to remove a class from a JAR. Instead, update the JAR.

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > External Environments > Java > JARs**.
3. Select one or more JAR files from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or

- From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple JAR files.

4. Review the confirmation dialog and click **Yes**.

See also

- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Updating a Java Classes File* on page 1191
- *Deleting a Classes File* on page 1192
- *Viewing or Modifying Java Classes File Properties* on page 1193
- *Installing a Java JAR File into an SAP Sybase IQ Database* on page 1194
- *Updating a Java JAR File* on page 1196
- *Viewing or Modifying the Java JAR File Properties* on page 1198
- *Testing the Configuration of a Java External Environment* on page 1200
- *Viewing or Modifying Java External Environment Properties* on page 1201
- *Java External Environment Privilege Summary* on page 1202
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying the Java JAR File Properties

Display the properties of a Java JAR file associated with a Sybase IQ database. Only the comment can be modified.

Prerequisites

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	View external environment properties – None required. Modify external environment properties – Requires DBA authority.
SAP Sybase IQ 16.0	View external environment properties – None required. Modify external environment properties – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments > Java > Classes**.

3. Select a class from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The Java Class Properties view appears.

4. Edit the comments field if needed. All other properties are read-only.

If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) Name of the class.</p> <p>Type – (Read-only) Type of class.</p> <p>Creator – (Read-only) User who created the class.</p> <p>Time created – (Read-only) Date and time the class file was created.</p> <p>Time modified – (Read-only) Date and time the class file was last modified.</p> <p>Comment – A text field for adding an optional comment about the class file.</p>
Classes (Read-only)	The list of classes contained within the JAR file.

5. Click **OK** to save any changes and closed the view.

See also

- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Updating a Java Classes File* on page 1191
- *Deleting a Classes File* on page 1192
- *Viewing or Modifying Java Classes File Properties* on page 1193
- *Installing a Java JAR File into an SAP Sybase IQ Database* on page 1194
- *Updating a Java JAR File* on page 1196
- *Deleting a JAR File* on page 1197
- *Testing the Configuration of a Java External Environment* on page 1200
- *Viewing or Modifying Java External Environment Properties* on page 1201
- *Java External Environment Privilege Summary* on page 1202
- *Authenticating a Login Account for a Managed Resource* on page 282

Testing the Configuration of a Java External Environment

Test the configuration of a Java external environment to make sure the JRE is accessible and responding.

Prerequisites

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires <code>MANAGE ANY EXTERNAL ENVIRONMENT</code> system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments**.
3. Select an external environment from the right pane and either:
 - Click the arrow to the right of the name and select **Test Configuration**, or
 - From the Administration Console menu bar, select **Resource > Test Configuration**.

The Test Configuration dialog displays progress messages to report stopping and then starting the external environment.

4. Click **Finish** to close the view.
- If the test fails because the `iq_java.sh` script in the Sybase IQ server's `bin` directory failed to execute, run the script manually to check for errors.
 - If the test fails because the JRE has been deleted or moved to a new location, use the **Updating Java a Classes File** or **Updating a Java Jar File** feature to specify a new location.

See also

- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Updating a Java Classes File* on page 1191
- *Deleting a Classes File* on page 1192
- *Viewing or Modifying Java Classes File Properties* on page 1193
- *Installing a Java JAR File into an SAP Sybase IQ Database* on page 1194
- *Updating a Java JAR File* on page 1196

- *Deleting a JAR File* on page 1197
- *Viewing or Modifying the Java JAR File Properties* on page 1198
- *Viewing or Modifying Java External Environment Properties* on page 1201
- *Java External Environment Privilege Summary* on page 1202
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Java External Environment Properties

Display and change the properties of a Java external environment, including the location of the executable and the associated user.

Prerequisites

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL ENVIRONMENT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments**.
3. Select a Java external environment from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The External Environment Properties view appears.

4. View or modify the properties.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Option	Description
Location	The path to the Java file.

Option	Description
User	The Sybase IQ user or role/group that the external environment uses to log in to the database. The user or role/group must have been granted DBA authority (15.x) or the MANAGE ANY EXTERNAL ENVIRONMENT system privilege (16.x).
Comment	Notes describing the external environment.

5. Click **Apply** to save your changes and keep editing, or click **OK** to save and close the properties dialog.

See also

- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Updating a Java Classes File* on page 1191
- *Deleting a Classes File* on page 1192
- *Viewing or Modifying Java Classes File Properties* on page 1193
- *Installing a Java JAR File into an SAP Sybase IQ Database* on page 1194
- *Updating a Java JAR File* on page 1196
- *Deleting a JAR File* on page 1197
- *Viewing or Modifying the Java JAR File Properties* on page 1198
- *Testing the Configuration of a Java External Environment* on page 1200
- *Java External Environment Privilege Summary* on page 1202
- *Authenticating a Login Account for a Managed Resource* on page 282

Java External Environment Privilege Summary

A list of the system privileges and object permissions required to complete the various external environment java tasks.

Installing a Java Classes or JAR File

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Updating a Java Classes or JAR File

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.

Database Version	External Environment – Java Privileges
SAP Sybase IQ 16.0	Requires <code>MANAGE ANY EXTERNAL OBJECT</code> system privilege.

Deleting a Java Classes or JAR File

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires <code>MANAGE ANY EXTERNAL OBJECT</code> system privilege.

Viewing or Modifying a Java Classes or JAR File

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	View external environment properties – None required. Modify external environment properties – Requires DBA authority.
SAP Sybase IQ 16.0	View external environment properties – None required. Modify external environment properties – Requires <code>MANAGE ANY EXTERNAL OBJECT</code> system privilege.

Testing the Configuration of a Java External Environment

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires <code>MANAGE ANY EXTERNAL ENVIRONMENT</code> system privilege.

Viewing or Modifying Java External Environment Properties

Database Version	External Environment – Java Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires <code>MANAGE ANY EXTERNAL ENVIRONMENT</code> system privilege.

See also

- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189

- *Updating a Java Classes File* on page 1191
- *Deleting a Classes File* on page 1192
- *Viewing or Modifying Java Classes File Properties* on page 1193
- *Installing a Java JAR File into an SAP Sybase IQ Database* on page 1194
- *Updating a Java JAR File* on page 1196
- *Deleting a JAR File* on page 1197
- *Viewing or Modifying the Java JAR File Properties* on page 1198
- *Testing the Configuration of a Java External Environment* on page 1200
- *Viewing or Modifying Java External Environment Properties* on page 1201

Working in a Perl External Environment

Install Perl objects, test a Perl external environment, and change its properties.

A Perl stored procedure or function behaves like a SQL stored procedure or function except that the code for the procedure or function is written in Perl and the execution of the procedure or function takes place outside the database server (that is, within a Perl executable instance).

You must create a separate instance of the Perl executable for each connection that uses Perl stored procedures and functions. This behavior is different from Java stored procedures and functions. For Java, there is one instance of the Java VM for each database rather than one instance per connection. The other major difference between Perl and Java is that Perl stored procedures do not return result sets, whereas Java stored procedures can return result sets.

See also

- *Working in a Java External Environment* on page 1189
- *Working in a PHP External Environment* on page 1215
- *Working in a C ESQL External Environment* on page 1226
- *Working in a C ODBC External Environment* on page 1228
- *Working in a CLR (.NET) External Environment* on page 1230

Creating a Perl Object

Install Perl and create a Perl object before installing the new Perl object into the SAP Sybase IQ database.

Prerequisites

- Install ActivePerl 5.6.0 on the database server computer. The database server computer must be able to locate the Perl executable.
- Install the DBI Perl module on the database server computer.
- Install the DBD : : SQLAnywhere driver on the database server computer.
- On Windows, install Microsoft Visual Studio and configure your environment.

Task

1. Run **Makefile.PL**:

- From the SDK\PerlEnv subdirectory (Windows):

```
perl Makefile.PL
nmake
nmake install
```

- From the sdk/perlenv subdirectory (UNIX):

```
perl Makefile.PL
make
make install
```

2. Verify that the database server is able to locate and start the Perl executable:

```
START EXTERNAL ENVIRONMENT PERL;
```

3. Write Perl scripts that use the DBD::SQLAnywhere interface. Sybase recommends running Perl in strict mode:

```
#!/usr/local/bin/perl -w
#
use DBI;
use strict;
my $database = "demo";
my $data_src = "DBI:SQLAnywhere:SERVER=$database;DBN=$database";
my $uid      = "DBA";
my $pwd      = "sql";
my %defaults = (
    AutoCommit => 1, # Autocommit enabled.
    PrintError => 0 # Errors not automatically printed.
);
my $dbh = DBI->connect($data_src, $uid, $pwd, \%defaults)
    or die "Cannot connect to $data_src: $DBI::errstr\n";
$dbh->disconnect;
exit(0);
__END__
```

See also

- Perl Objects in SQL Procedures and Functions* on page 1206
- Installing a Perl Object into an SAP Sybase IQ Database* on page 1206
- Updating a Perl Object* on page 1208
- Deleting a Perl Object* on page 1209
- Viewing or Modifying Perl Object Properties.* on page 1210
- Testing the Configuration of a Perl External Environment* on page 1211
- Viewing or Modifying Perl External Environment Properties* on page 1212
- Perl External Environment Privilege Summary* on page 1214

Perl Objects in SQL Procedures and Functions

When defining SQL procedures and functions referencing Perl objects, the **LANGUAGE** is always *PERL* and the **EXTERNAL NAME** string contains the information needed to call the Perl subroutines and to return **OUT** parameters and return values.

In this example, the Perl object PerlConsoleExample creates the string 'Hello world'. This SQL procedure writes the output of PerlConsoleExample to the database server messages window:

```
CREATE PROCEDURE PerlWriteToConsole( IN str LONG VARCHAR)
  EXTERNAL NAME '<file=PerlConsoleExample>
    WriteToServerConsole( $sa_perl_arg0 )'
  LANGUAGE PERL;

// 'Hello world' should appear in the database server messages window
CALL PerlWriteToConsole( 'Hello world' );
```

See also

- *Creating a Perl Object* on page 1204
- *Installing a Perl Object into an SAP Sybase IQ Database* on page 1206
- *Updating a Perl Object* on page 1208
- *Deleting a Perl Object* on page 1209
- *Viewing or Modifying Perl Object Properties.* on page 1210
- *Testing the Configuration of a Perl External Environment* on page 1211
- *Viewing or Modifying Perl External Environment Properties* on page 1212
- *Perl External Environment Privilege Summary* on page 1214

Installing a Perl Object into an SAP Sybase IQ Database

Install a Perl object into an SAP Sybase IQ database. After installing it, you can reference the object in SQL procedures and functions.

Prerequisites

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires <code>MANAGE ANY EXTERNAL OBJECT</code> system privilege.

- The SAP Sybase IQ resource is authenticated and running.

A Perl external environment appears in the list of external environments in the Sybase Control Center Administration Console even when no Perl objects have been installed.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments > Perl**.
3. Click the arrow beside Perl and select **New**.
The Install Perl Object wizard appears.
4. On the Welcome page, specify:

Option	Description
Select an SAP Sybase IQ resource on which the Perl object will be installed:	Select an SAP Sybase IQ resource from the list.
(Multiplex only) Select a multiplex server on which the Perl object will be installed	Select a multiplex server from the list.
SCC agent status	Indicates the current status of the SCC agent. If the SCC agent is not registered, click Register Agent and enter the required registration information. If the SCC agent is not authenticated, click Authenticate Agent . Enter a user ID, password, and port for SCC to use when it logs in to the SCC agent.
Perl script path	Enter the path to the Perl object. It must be on a file system accessible to the SAP Sybase IQ resource.
Perl object name in the database	Enter the Perl object name.
Comment	(Optional) Enter a comment describing the Perl object.

5. Click **Finish** to install the Perl object.

See also

- *Creating a Perl Object* on page 1204
- *Perl Objects in SQL Procedures and Functions* on page 1206
- *Updating a Perl Object* on page 1208
- *Deleting a Perl Object* on page 1209
- *Viewing or Modifying Perl Object Properties.* on page 1210
- *Testing the Configuration of a Perl External Environment* on page 1211

- *Viewing or Modifying Perl External Environment Properties* on page 1212
- *Perl External Environment Privilege Summary* on page 1214
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Registering and Authenticating a Sybase Control Center Agent* on page 279

Updating a Perl Object

Update a Perl object in a Sybase IQ database.

Prerequisites

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- Put an updated version of the Perl object in a location accessible to the Sybase IQ server.

Task

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > External Environments > Java > Perl**.
3. Select a Perl object from the right pane and either:
 - Click the arrow to the right of the name and select **Update**, or
 - From the Administration Console menu bar, select **Properties > Update**.

The Update External Environment Object view appears.

4. On the Update Class page, if the **Register Agent** button is active, click it to register the SCC agent on the Perl object's Sybase IQ server. Enter the required registration information.
5. If the **Authenticate Agent** button is active, click it to authenticate the SCC agent. Enter a user ID and password for SCC to use when it logs in to the SCC agent.
6. Enter the path to the updated Perl object. It must be on a file system accessible to the Sybase IQ resource.
7. Click **Next**.
8. Click **Finish**.

See also

- *Creating a Perl Object* on page 1204
- *Perl Objects in SQL Procedures and Functions* on page 1206

- *Installing a Perl Object into an SAP Sybase IQ Database* on page 1206
- *Deleting a Perl Object* on page 1209
- *Viewing or Modifying Perl Object Properties.* on page 1210
- *Testing the Configuration of a Perl External Environment* on page 1211
- *Viewing or Modifying Perl External Environment Properties* on page 1212
- *Perl External Environment Privilege Summary* on page 1214
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Registering and Authenticating a Sybase Control Center Agent* on page 279

Deleting a Perl Object

Remove a JAR file from an SAP Sybase IQ database.

Prerequisites

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > External Environments > Java > Perl**.
3. Select one or more Perl objects from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple Perl objects.

4. Review the confirmation dialog and click **Yes**.

See also

- *Creating a Perl Object* on page 1204
- *Perl Objects in SQL Procedures and Functions* on page 1206
- *Installing a Perl Object into an SAP Sybase IQ Database* on page 1206
- *Updating a Perl Object* on page 1208
- *Viewing or Modifying Perl Object Properties.* on page 1210
- *Testing the Configuration of a Perl External Environment* on page 1211

- *Viewing or Modifying Perl External Environment Properties* on page 1212
- *Perl External Environment Privilege Summary* on page 1214
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Perl Object Properties.

Display the properties of a Perl object associated with an SAP Sybase IQ database. Only the comment can be modified.

Prerequisites

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	View external environment properties – None required. Modify View external environment properties – Requires DBA authority.
SAP Sybase IQ 16.0	View external environment properties – None required. Modify external environment properties – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments > Perl**.
3. Select a Perl object from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The External Environment Object Properties view appears.

4. Edit the comments field if needed. All other properties are read-only.

If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) Name of the perl object.</p> <p>Type – (Read-only) Type of Perl object.</p> <p>Creator – (Read-only) User who created the Perl object.</p> <p>External environment – (Read-only) External environment of the Perl object</p> <p>Time modified – (Read-only) Date and time the Perl object was last modified.</p> <p>Comment – A text field for adding an optional comment about the Perl object.</p>
Content (Read-only)	The content of the Perl script.

5. Click **OK** to save any changes and closed the view.

See also

- *Creating a Perl Object* on page 1204
- *Perl Objects in SQL Procedures and Functions* on page 1206
- *Installing a Perl Object into an SAP Sybase IQ Database* on page 1206
- *Updating a Perl Object* on page 1208
- *Deleting a Perl Object* on page 1209
- *Testing the Configuration of a Perl External Environment* on page 1211
- *Viewing or Modifying Perl External Environment Properties* on page 1212
- *Perl External Environment Privilege Summary* on page 1214
- *Authenticating a Login Account for a Managed Resource* on page 282

Testing the Configuration of a Perl External Environment

Test the configuration of a Perl external environment to make sure the Perl object is accessible and responding.

Prerequisites

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments**.
3. Select an external environment from the right pane and either:
 - Click the arrow to the right of the name and select **Test Configuration**, or
 - From the Administration Console menu bar, select **Resource > Test Configuration**.

The Test Configuration dialog displays progress messages to report stopping and then starting the external environment.

4. Click **Finish** to close the view.
- If the text fails because the Perl object has been deleted or moved to a new location, use the **Updating a Perl Object** feature to specify a new location.

See also

- *Creating a Perl Object* on page 1204
- *Perl Objects in SQL Procedures and Functions* on page 1206
- *Installing a Perl Object into an SAP Sybase IQ Database* on page 1206
- *Updating a Perl Object* on page 1208
- *Deleting a Perl Object* on page 1209
- *Viewing or Modifying Perl Object Properties* on page 1210
- *Viewing or Modifying Perl External Environment Properties* on page 1212
- *Perl External Environment Privilege Summary* on page 1214
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Perl External Environment Properties

Display and change the properties of a Perl external environment, including the location of the Perl object and the associated user.

Prerequisites

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments**.
3. Select a Perl external environment from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The External Environment Properties view appears.

4. View or modify the properties.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.
5. In the properties dialog, modify any of these:

Option	Description
Location	The path to the Perl object.
User	The SAP Sybase IQ user or role/group that the external environment uses to log in to the database. The user or role/group must have been granted DBA authority (15.x) or the MANAGE ANY EXTERNAL ENVIRONMENT system privilege (16.x).
Comment	Notes describing the external environment.

6. Click **Apply** to save your changes and keep editing, or click **OK** to save and close the properties dialog.

See also

- *Creating a Perl Object* on page 1204
- *Perl Objects in SQL Procedures and Functions* on page 1206
- *Installing a Perl Object into an SAP Sybase IQ Database* on page 1206
- *Updating a Perl Object* on page 1208
- *Deleting a Perl Object* on page 1209

- *Viewing or Modifying Perl Object Properties.* on page 1210
- *Testing the Configuration of a Perl External Environment* on page 1211
- *Perl External Environment Privilege Summary* on page 1214
- *Authenticating a Login Account for a Managed Resource* on page 282

Perl External Environment Privilege Summary

A list of the system privileges and object permissions required to complete the various Perl external environment tasks.

Installing a Perl Object

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Updating a Perl Object

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Deleting a Perl Object

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Viewing or Modifying a Perl Object Properties

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	View external environment properties – None required. Modify View external environment properties – Requires DBA authority.
SAP Sybase IQ 16.0	View external environment properties – None required. Modify external environment properties – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Testing the Configuration of a Perl External Environment

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires <code>MANAGE ANY EXTERNAL OBJECT</code> system privilege.

Viewing or Modifying Perl External Environment Properties

Database Version	External Environment – Perl Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires <code>MANAGE ANY EXTERNAL OBJECT</code> system privilege.

See also

- *Creating a Perl Object* on page 1204
- *Perl Objects in SQL Procedures and Functions* on page 1206
- *Installing a Perl Object into an SAP Sybase IQ Database* on page 1206
- *Updating a Perl Object* on page 1208
- *Deleting a Perl Object* on page 1209
- *Viewing or Modifying Perl Object Properties.* on page 1210
- *Testing the Configuration of a Perl External Environment* on page 1211
- *Viewing or Modifying Perl External Environment Properties* on page 1212

Working in a PHP External Environment

Install PHP objects, test a PHP external environment, and change its properties.

A PHP stored procedure or function behaves the same as a SQL stored procedure or function except that the code for the procedure or function is written in PHP and the execution of the procedure or function takes place outside the database server (that is, within a PHP executable instance).

You must create a separate instance of the PHP executable for each connection that uses PHP stored procedures and functions. This behavior is quite different from Java stored procedures and functions. For Java, there is one instance of the Java VM for each database rather than one instance per connection. The other major difference between PHP and Java is that PHP stored procedures do not return result sets, whereas Java stored procedures can return result sets. PHP only returns an object of type `LONG VARCHAR`, which is the output of the PHP script.

See also

- *Working in a Java External Environment* on page 1189
- *Working in a Perl External Environment* on page 1204
- *Working in a C ESQL External Environment* on page 1226
- *Working in a C ODBC External Environment* on page 1228
- *Working in a CLR (.NET) External Environment* on page 1230

Creating a PHP Object

Install PHP and create a PHP script before installing the new PHP object into the SAP Sybase IQ database.

Prerequisites

- Install PHP on the database server computer. The database server computer must be able to locate the PHP executable.
- Install the SQL Anywhere PHP extension on the database server computer.

Task

1. Locate the `php.ini` file for your PHP installation, and open it in a text editor. Locate the line that specifies the location of the `extension_dir` directory. If `extension_dir` is not set to any specific directory, it is a good idea to set it to point to an isolated directory for better system security.
2. Copy the desired external environment PHP module from the SAP Sybase IQ installation directory to your PHP installation directory. Change the `x.y` to reflect the version you have selected.

```
cp $SQLANY12/bin32/php-5.x.y_sqlanywhere_extenv12.so  
php-dir/ext
```

3. Add the following line to the Dynamic Extensions section of the `php.ini` file to load the external environment PHP module automatically. Change the `x.y` to reflect the version you have selected.

```
extension=php-5.x.y_sqlanywhere_extenv12.so
```

Save and close `php.ini`.

4. Make sure that you have also installed the SQL Anywhere PHP driver from the SAP Sybase IQ installation directory into your PHP extensions directory. This file name follows the pattern `php-5.x.y_sqlanywhere.so` where `x` and `y` are the version numbers.
5. Verify the database server can locate and start the PHP executable:

```
ALTER EXTERNAL ENVIRONMENT PHP  
LOCATION 'php-path';
```


6. Write your PHP script. The `<?php` and `?>` tags tell the web server that it should let PHP execute the code that lies between them and replace it with the PHP output. This `connect.php` example attempts to make a connection to a database on a local server:

```
<?php
# Connect using the default user ID and password
$conn = sasql_connect( "UID=DBA;PWD=sql" );
if( ! $conn ){
    echo "Connection failed\n";
} else {
    echo "Connected successfully\n";
    sasql_close( $conn );
}??>
```

See also

- *Installing a PHP Object* on page 1217
- *Updating a PHP Object* on page 1219
- *Deleting a PHP Object* on page 1220
- *Viewing or Modifying PHP Object Properties* on page 1221
- *Testing the Configuration of a PHP External Environment* on page 1222
- *Viewing or Modifying PHP External Environment Properties* on page 1223
- *PHP External Environment Privilege Summary* on page 1225

Installing a PHP Object

Install a PHP object into an SAP Sybase IQ database. After installing it, you can reference the object in SQL procedures and functions.

Prerequisites

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	View external environment properties – None required. Modify external environment properties – Requires DBA authority.
SAP Sybase IQ 16.0	View external environment properties – None required. Modify external environment properties – Requires <code>MANAGE ANY EXTERNAL OBJECT</code> system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

A PHP external environment appears in the list of external environments in the Sybase Control Center Administration Console even when no PHP objects have been installed.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments > PHP**.
3. Click the arrow beside PHP and select **New**.
The Install PHP Object wizard appears.
4. On the Welcome page, specify:

Option	Description
Select an SAP Sybase IQ resource on which the PHP object will be installed:	Select an SAP Sybase IQ resource from the list.
(Multiplex only) Select a multiplex server on which the PHP object will be installed	Select a multiplex server from the list.
SCC agent status	Indicates the current status of the SCC agent. If the SCC agent is not registered, click Register Agent and enter the required registration information. If the SCC agent is not authenticated, click Authenticate Agent . Enter a user ID, password, and port for SCC to use when it logs in to the SCC agent.
PHP script path	Enter the path to the PHP object. It must be on a file system accessible to the SAP Sybase IQ resource.
PHP object name in the database	Enter the PHP object name.
Comment	(Optional) Enter a comment describing the PHP object.

5. Click **Finish** to install the PHP object.

See also

- *Creating a PHP Object* on page 1216
- *Updating a PHP Object* on page 1219
- *Deleting a PHP Object* on page 1220
- *Viewing or Modifying PHP Object Properties* on page 1221
- *Testing the Configuration of a PHP External Environment* on page 1222
- *Viewing or Modifying PHP External Environment Properties* on page 1223
- *PHP External Environment Privilege Summary* on page 1225
- *Authenticating a Login Account for a Managed Resource* on page 282

- *Registering and Authenticating a Sybase Control Center Agent* on page 279

Updating a PHP Object

Update a PHP object in an SAP Sybase IQ database.

Prerequisites

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- Put an updated version of the PHP object in a location accessible to the Sybase IQ server.

Task

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > External Environments > Java > PHP**.
3. Select a PHP object from the right pane and either:
 - Click the arrow to the right of the name and select **Update**, or
 - From the Administration Console menu bar, select **Properties > Update**.

The Update External Environment Object view appears.

4. On the Update PHP Object page, if the **Register Agent** button is active, click it to register the SCC agent on the SAP Sybase IQ server. Enter the required registration information.
5. If the **Authenticate Agent** button is active, click it to authenticate the SCC agent. Enter a user ID and password for SCC to use when it logs in to the SCC agent.
6. Enter the path to the updated PHP object. It must be on a file system accessible to the SAP Sybase IQ resource.
7. Click **Next**.
8. Click **Finish**.

See also

- *Creating a PHP Object* on page 1216
- *Installing a PHP Object* on page 1217
- *Deleting a PHP Object* on page 1220
- *Viewing or Modifying PHP Object Properties* on page 1221
- *Testing the Configuration of a PHP External Environment* on page 1222

- *Viewing or Modifying PHP External Environment Properties* on page 1223
- *PHP External Environment Privilege Summary* on page 1225
- *Authenticating a Login Account for a Managed Resource* on page 282
- *Registering and Authenticating a Sybase Control Center Agent* on page 279

Deleting a PHP Object

Remove a PHP object from an SAP Sybase IQ database.

Prerequisites

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > External Environments > Java > PHP**.
3. Select one or more PHP objects from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple PHP objects.

4. Review the confirmation dialog and click **Yes**.

See also

- *Creating a PHP Object* on page 1216
- *Installing a PHP Object* on page 1217
- *Updating a PHP Object* on page 1219
- *Viewing or Modifying PHP Object Properties* on page 1221
- *Testing the Configuration of a PHP External Environment* on page 1222
- *Viewing or Modifying PHP External Environment Properties* on page 1223
- *PHP External Environment Privilege Summary* on page 1225
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying PHP Object Properties

Display the properties of a PHP object associated with an SAP Sybase IQ database. Only the comment can be modified.

Prerequisites

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	View properties – None required. Modify comment – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments > PHP**.
3. Select a PHP object from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The PHP Object Properties view appears.

4. Edit the comments field if needed. All other properties are read-only.

If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) Name of the PHP object.</p> <p>Type – (Read-only) Type of PHP object.</p> <p>Creator – (Read-only) User who created the PHP object.</p> <p>External environment – (Read-only) External environment of the PHP object</p> <p>Time modified – (Read-only) Date and time the PHP object was last modified.</p> <p>Comment – A text field for adding an optional comment about the PHP object.</p>
Content (Read-only)	The content of the PHP script.

5. Click **OK** to save any changes and closed the view.

See also

- *Creating a PHP Object* on page 1216
- *Installing a PHP Object* on page 1217
- *Updating a PHP Object* on page 1219
- *Deleting a PHP Object* on page 1220
- *Testing the Configuration of a PHP External Environment* on page 1222
- *Viewing or Modifying PHP External Environment Properties* on page 1223
- *PHP External Environment Privilege Summary* on page 1225
- *Authenticating a Login Account for a Managed Resource* on page 282

Testing the Configuration of a PHP External Environment

Test the configuration of a PHP external environment to make sure the PHP object is accessible and responding.

Prerequisites

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments**.
3. Select an external environment from the right pane and either:
 - Click the arrow to the right of the name and select **Test Configuration**, or
 - From the Administration Console menu bar, select **Resource > Test Configuration**.

The Test Configuration dialog displays progress messages to report stopping and then starting the external environment.

4. Click **Finish** to close the view.
- If the text fails because the PHP object has been deleted or moved to a new location, use the **Updating a PHP Object** feature to specify a new location.

See also

- *Creating a PHP Object* on page 1216
- *Installing a PHP Object* on page 1217
- *Updating a PHP Object* on page 1219
- *Deleting a PHP Object* on page 1220
- *Viewing or Modifying PHP Object Properties* on page 1221
- *Viewing or Modifying PHP External Environment Properties* on page 1223
- *PHP External Environment Privilege Summary* on page 1225
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying PHP External Environment Properties

Display and change the properties of a PHP external environment, including the location of the PHP object and the associated user.

Prerequisites

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments**.
3. Select a PHP external environment from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The External Environment Properties view appears.

4. Select **Properties**.
5. In the properties dialog, modify any of these:

Option	Description
Location	The path to the PHP object.
User	The SAP Sybase IQ user or role/group that the external environment uses to log in to the database. The user or role/group must have been granted DBA authority (15.x) or the MANAGE ANY EXTERNAL ENVIRONMENT system privilege (16.x).
Comment	Notes describing the external environment.

6. Click **Apply** to save your changes and keep editing, or click **OK** to save and close the properties dialog.

See also

- *Creating a PHP Object* on page 1216
- *Installing a PHP Object* on page 1217
- *Updating a PHP Object* on page 1219
- *Deleting a PHP Object* on page 1220
- *Viewing or Modifying PHP Object Properties* on page 1221
- *Testing the Configuration of a PHP External Environment* on page 1222
- *PHP External Environment Privilege Summary* on page 1225
- *Authenticating a Login Account for a Managed Resource* on page 282

PHP External Environment Privilege Summary

A list of the system privileges and object permissions required to complete the various PHP external environment tasks.

Installing a PHP Object

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	View external environment properties – None required. Modify external environment properties – Requires DBA authority.
SAP Sybase IQ 16.0	View external environment properties – None required. Modify external environment properties – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Updating a PHP Object

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Deleting a PHP Object

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Viewing or Modifying a PHP Object Properties

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	View properties – None required. Modify comment – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Testing the Configuration of a PHP External Environment

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY EXTERNAL OBJECT system privilege.

Viewing or Modifying PHP External Environment Properties

Database Version	External Environment – PHP Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page– None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

See also

- *Creating a PHP Object* on page 1216
- *Installing a PHP Object* on page 1217
- *Updating a PHP Object* on page 1219
- *Deleting a PHP Object* on page 1220
- *Viewing or Modifying PHP Object Properties* on page 1221
- *Testing the Configuration of a PHP External Environment* on page 1222
- *Viewing or Modifying PHP External Environment Properties* on page 1223

Working in a C ESQL External Environment

View and update the properties of C ESQL32 and C ESQL64 external environments.

Install the C or C++ code outside of SCC. You cannot use SCC to install the executable.

See also

- *Working in a Java External Environment* on page 1189
- *Working in a Perl External Environment* on page 1204
- *Working in a PHP External Environment* on page 1215
- *Working in a C ODBC External Environment* on page 1228
- *Working in a CLR (.NET) External Environment* on page 1230

Viewing or Modifying C ESQL Executable Properties

Display and change the properties of a C ESQL32 or C ESQL64 external environment, including the location of the executable and the associated user.

Prerequisites

Database Version	Other External Environment Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments**.
3. Select a C ESQL32 or C ESQL64 external environment from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
4. In the properties dialog, modify any of these:

Option	Description
Location	The path to the C ESQL32 or C ESQL64 executable.
User	The Sybase IQ user or role/group that the external environment uses to log in to the database. The user or role/group must have been granted DBA authority (15.x) or the MANAGE ANY EXTERNAL ENVIRONMENT system privilege (16.x).
Comment	Notes describing the external environment.

5. Click **Apply** to save your changes and keep editing, or click **OK** to save and close the properties dialog.

See also

- *Other External Environment Privilege Summary* on page 1228
- *Authenticating a Login Account for a Managed Resource* on page 282

Other External Environment Privilege Summary

A list of the system privileges and object permissions required to complete the various external environment tasks.

Viewing or Modifying C ESQL, C ODBC, or CLR (.NET) Executable Properties

Database Version	Other External Environment Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

See also

- *Viewing or Modifying C ESQL Executable Properties* on page 1227

Working in a C ODBC External Environment

View and update the properties of C ODBC32 and C ODBC64 external environments.

Install the C or C++ code outside of SCC. You cannot use SCC to install the executable.

See also

- *Working in a Java External Environment* on page 1189
- *Working in a Perl External Environment* on page 1204
- *Working in a PHP External Environment* on page 1215
- *Working in a C ESQL External Environment* on page 1226
- *Working in a CLR (.NET) External Environment* on page 1230

Viewing or Modifying C ODBC Executable Properties

Display and change the properties of a C ODBC32 or C ODBC64 external environment, including the location of the executable and the associated user.

Prerequisites

Database Version	Other External Environment Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.

Database Version	Other External Environment Privileges
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments**.
3. Select a C ODBC32 or C ODBC64 external environment from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
4. In the properties dialog, modify any of these:

Option	Description
Location	The path to the C ODBC32 or C ODBC64 executable.
User	The Sybase IQ user or role/group that the external environment uses to log in to the database. The user or role/group must have been granted DBA authority (15.x) or the MANAGE ANY EXTERNAL ENVIRONMENT system privilege (16.x).
Comment	Notes describing the external environment.

5. Click **Apply** to save your changes and keep editing, or click **OK** to save and close the properties dialog.

See also

- *Other External Environment Privilege Summary* on page 1230
- *Authenticating a Login Account for a Managed Resource* on page 282

Other External Environment Privilege Summary

A list of the system privileges and object permissions required to complete the various external environment tasks.

Viewing or Modifying C ESQL, C ODBC, or CLR (.NET) Executable Properties

Database Version	Other External Environment Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

See also

- *Viewing or Modifying C ODBC Executable Properties* on page 1228

Working in a CLR (.NET) External Environment

View and update the properties of a CLR external environment.

The CLR external environment is supported on Windows servers only.

Install the .NET code outside of SCC. You cannot use SCC to install the executable.

See also

- *Working in a Java External Environment* on page 1189
- *Working in a Perl External Environment* on page 1204
- *Working in a PHP External Environment* on page 1215
- *Working in a C ESQL External Environment* on page 1226
- *Working in a C ODBC External Environment* on page 1228

Viewing or Modifying CLR (.NET) Executable Properties

Display and change the properties of a CLR external environment, including the location of the executable and the associated user.

Prerequisites

Database Version	Other External Environment Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.

Database Version	Other External Environment Privileges
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires MANAGE ANY EXTERNAL OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > External Environments**.
3. Select a CLR (.NET) external environment from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.
4. In the properties dialog, modify any of these:

Option	Description
Location	The path to the .NET executable.
User	The Sybase IQ user or role/group that the external environment uses to log in to the database. The user or role/group must have been granted DBA authority (15.x) or the MANAGE ANY EXTERNAL ENVIRONMENT system privilege (16.x).
Comment	Notes describing the external environment.

5. Click **Apply** to save your changes and keep editing, or click **OK** to save and close the properties dialog.

See also

- *Other External Environment Privilege Summary* on page 1232
- *Authenticating a Login Account for a Managed Resource* on page 282

Other External Environment Privilege Summary

A list of the system privileges and object permissions required to complete the various external environment tasks.

Viewing or Modifying C ESQL, C ODBC, or CLR (.NET) Executable Properties

Database Version	Other External Environment Privileges
SAP Sybase IQ 15.3 and 15.4	View any external environment property page – None required. Modify any external environment property – Requires DBA authority.
SAP Sybase IQ 16.0	View any external environment property page – None required. Modify any external environment property – Requires <code>MANAGE ANY EXTERNAL OBJECT</code> system privilege.

See also

- *Viewing or Modifying CLR (.NET) Executable Properties* on page 1230

Functions

Create, delete, display, and manage the properties of functions in SAP Sybase IQ.

Sample functions and procedures are provided with SAP Sybase IQ. Sample functions are visible in Sybase Control Center in the Administration Console (**IQ Servers > Compiled Objects > Functions**). The samples include explanatory comments and can be found in `IQ-X_X/samples/udf`, where `X_X` is the SAP Sybase IQ release number (16.0, for example).

Creating a Watcom SQL or Transact-SQL Function

Set up a new Watcom SQL or Transact-SQL function on an SAP Sybase IQ server.

Prerequisites

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Watcom SQL or Transact-SQL function to be owned by self – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE ADMIN authority. <p>Watcom SQL or Transact-SQL function to be owned by any user –</p> <ul style="list-style-type: none"> • Requires DBA authority.
SAP Sybase IQ 16.0	<p>Watcom SQL or Transact-SQL to be owned by self –</p> <ul style="list-style-type: none"> • Requires CREATE PROCEDURE system privilege. <p>Watcom SQ or Transact-SQL function to be owned by any user –</p> <p>Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Functions**.
3. Click the arrow next to **Functions** and select **New**.
The Create Function Wizard appears.
4. On the Welcome page, specify:

Option	Description
Select a resource for which the function will be created	From the list, select the resource for which the function will be created.

Option	Description
Which user or group/role do you want to own the function?	From the list, select the user or role/group to own the function.
What do you want to name the function?	Enter a unique name for the new function; maximum of 128 characters.
Which SQL dialect or language do you want to use?	Select Watcom-SQL or Transact-SQL.
Use SQL template	(Optional) Select to insert a hardcoded SQL template and skip the wizard page for specifying a return type. You can also set a Watcom SQL function to be deterministic or nondeterministic.

5. Click **Next**.
6. If you chose to use the SQL template, skip to step 8. Otherwise, on the Specify Return Type page, select the type of value to return and define a name for the return variable.
7. Click **Next**.
8. On the SQL page, edit the code provided by the wizard.
 - a) Define input parameters: name, type, and default value.
 - b) Enter function statements.
 - c) Make any other changes needed to complete your function.
 - d) (Optional) Enter a comment describing the function.
 Comments can include both HTML and Javadoc tags, so you can incorporate them into your generated database documentation.
9. Click **Finish**.

See also

- *Creating an External Java Function* on page 1235
- *Creating an External C/C++ Scalar or Aggregate Function* on page 1237
- *Deleting a Function* on page 1239
- *Generating Function DDL Commands* on page 1240
- *Viewing and Modifying a Function* on page 1241
- *Granting Function EXECUTE Permission* on page 1244
- *Revoking Function EXECUTE Permission* on page 1245
- *Function Privilege Summary* on page 1246
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating an External Java Function

Set up a new external Java function on an SAP Sybase IQ server.

Prerequisites

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	External Java function to be owned by self or any user – Requires DBA authority.
SAP Sybase IQ 16.0	<p>External Java function to be owned by self –</p> <p>Requires all of:</p> <ul style="list-style-type: none"> • CREATE PROCEDURE system privilege. • CREATE EXTERNAL REFERENCE system privilege. <p>External Java function to be owned by any user –</p> <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- (Optional) Install the required Java classes and JAR files in the database. (You can create the function if the classes and JAR files are not installed, but SAP Sybase IQ cannot execute the function.)

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Functions**.
3. Click the arrow next to **Functions** and select **New**.
The Create Function Wizard appears.
4. On the Welcome page, specify:

Option	Description
Select a resource for which the function will be created	From the list, select the resource for which the function will be created.

Option	Description
Which user or group/role do you want to own the function?	From the list, select the user or role/group to own the function.
What do you want to name the function?	Enter a unique name for the new function; maximum of 128 characters.
Which SQL dialect or language do you want to use?	Select External Java.
Use SQL template	(Optional) Select to insert a hardcoded SQL template and skip the wizard page for specifying a return type. You can also set a Watcom SQL function to be deterministic or nondeterministic.

5. Click **Next**.
6. If you chose to use the SQL template, skip to step 8. Otherwise, on the Specify Return Type page, select the type of value to return and define a name for the return variable.
7. Click **Next**.
8. On the SQL page, edit the code provided by the wizard.
 - a) Define input parameters: name, type, and default value.
 - b) If you chose to use the SQL template, replace the placeholder external name at the end of the query with a real name that follows the format of the placeholder.
 - c) Make any other changes needed to complete your function.
 - d) (Optional) Enter a comment describing the function.
 Comments can include both HTML and Javadoc tags, so you can incorporate them into your generated database documentation.
9. Click **Finish**.

See also

- *Creating a Watcom SQL or Transact-SQL Function* on page 1233
- *Creating an External C/C++ Scalar or Aggregate Function* on page 1237
- *Deleting a Function* on page 1239
- *Generating Function DDL Commands* on page 1240
- *Viewing and Modifying a Function* on page 1241
- *Granting Function EXECUTE Permission* on page 1244
- *Revoking Function EXECUTE Permission* on page 1245
- *Function Privilege Summary* on page 1246
- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating an External C/C++ Scalar or Aggregate Function

Set up a new external C or C++ aggregate function on an SAP Sybase IQ server.

Prerequisites

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	External C/C++ Scalar or Aggregate function to be owned by self or any user – <ul style="list-style-type: none"> • Requires DBA authority.
SAP Sybase IQ 16.0	External C/C++ Scalar or Aggregate function to be owned by self – Requires all of: <ul style="list-style-type: none"> • CREATE PROCEDURE system privilege. • CREATE EXTERNAL REFERENCE system privilege. External C/C++ Scalar or Aggregate function to be owned by any user – <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- You are licensed for the InDatabase Analytics Option (IQ_IDA).
- (Optional) Copy the library that contains the external function to a location accessible to the SAP Sybase IQ server. (You can create the function if the library is not accessible to SAP Sybase IQ, but SAP Sybase IQ cannot execute the function.)

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Functions**.
3. Click the arrow next to **Functions** and select **New**.
The Create Function Wizard appears.
4. On the Welcome page, specify:

Option	Description
Select a resource for which the function will be created	From the list, select the resource for which the function will be created.
Which user or group/role do you want to own the function?	From the list, select the user or role/group to own the function.
What do you want to name the function?	Enter a unique name for the new function; maximum of 128 characters.
Which SQL dialect or language do you want to use?	Select External C/C++ scalar or External C/C++ aggregate.
Use SQL template	(Optional) Select to insert a hardcoded SQL template and skip the wizard page for specifying a return type. You can also set a Watcom SQL function to be deterministic or nondeterministic.

5. Click **Next**.
6. If you chose to use the SQL template, skip to step 12. Otherwise, on the Specify Return Type page, select the type of value to return and whether to create a deterministic function.
7. Click **Next**.
8. On the Function Attributes page, specify the attributes of the function, including the names of its shared library file and descriptor function.
9. Click **Next**.
10. For External C/C++ aggregate only, on the Function Clauses page, configure clauses that control windows on the Function Clauses page.
11. Click **Next**.
12. On the SQL page, edit the code provided by the wizard.
 - a) Define input parameters: name, type, and default value.
 - b) If you chose to use the SQL template, replace the placeholder external name at the end of the query with a real name of the form `functionDescriptorName@libraryName`.
 - c) Make any other changes needed to complete your function.
 - d) (Optional) Enter a comment describing the function.
Comments can include both HTML and Javadoc tags, so you can incorporate them into your generated database documentation.
13. Click **Finish**.

See also

- *Creating a Watcom SQL or Transact-SQL Function* on page 1233

- *Creating an External Java Function* on page 1235
- *Deleting a Function* on page 1239
- *Generating Function DDL Commands* on page 1240
- *Viewing and Modifying a Function* on page 1241
- *Granting Function EXECUTE Permission* on page 1244
- *Revoking Function EXECUTE Permission* on page 1245
- *Function Privilege Summary* on page 1246
- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Function

Remove a function from an SAP Sybase IQ server.

Prerequisites

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You own the function.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY PROCEDURE system privilege. • DROP ANY OBJECT system privilege. • You own the function.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Functions**.
3. Select one or more functions from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple functions.

4. Click **Yes** to confirm deletion.

See also

- *Creating a Watcom SQL or Transact-SQL Function* on page 1233
- *Creating an External Java Function* on page 1235
- *Creating an External C/C++ Scalar or Aggregate Function* on page 1237
- *Generating Function DDL Commands* on page 1240
- *Viewing and Modifying a Function* on page 1241
- *Granting Function EXECUTE Permission* on page 1244
- *Revoking Function EXECUTE Permission* on page 1245
- *Function Privilege Summary* on page 1246
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Function DDL Commands

Generate the data description language for creating a function on an SAP Sybase IQ server. The DDL code can be a useful reference and training tool.

Prerequisites

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Functions**.
3. Select one or more functions from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple functions.

The DDL view shows the SQL code used to add the selected functions.

See also

- *Creating a Watcom SQL or Transact-SQL Function* on page 1233
- *Creating an External Java Function* on page 1235
- *Creating an External C/C++ Scalar or Aggregate Function* on page 1237

- *Deleting a Function* on page 1239
- *Viewing and Modifying a Function* on page 1241
- *Granting Function EXECUTE Permission* on page 1244
- *Revoking Function EXECUTE Permission* on page 1245
- *Function Privilege Summary* on page 1246
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing and Modifying a Function

View and change the SQL statement and properties of a function on an SAP Sybase IQ server.

Prerequisites

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any function property page regardless of type – None required.</p> <p>Modify permissions for any function type – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object. <p>Modify any other function property regardless of type – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the function.

Database Version	Function Privileges
SAP Sybase IQ 16.0	<p>View any function property page regardless of type – None required.</p> <p>Modify SQL code for Watcom SQL or Transact-SQL function – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the function. <p>Modify SQL code for External C/C++ Scalar or Aggregate, or External Java function – Requires one of:</p> <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the function. <p>Modify a comment for any function type – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • ALTER ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the function. <p>Modify permissions for any function type – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Functions**.
3. Select a function from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Function Properties view appears.

4. View or modify the properties.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) The name of the function.</p> <p>Owner – (Read-only) The owner of the function.</p> <p>Creation Time – (Read-only) The date and time the function was created.</p> <p>Dialect – (Read-only) The dialect of the function. Valid values are:</p> <ul style="list-style-type: none"> • Watcom-SQL • Transact-SQL • External C/C++ scalar • External C/C++ aggregate • External Java <p>Comment – A text field for adding an optional comment about the function.</p>
Parameters (Read-only)	The parameters defined from the function.
SQL	The SQL code to be executed by the function.
Permissions	See <i>Granting Function EXECUTE Permission</i> on page 1244 and <i>Revoking Function EXECUTE Permission</i> on page 1245

5. Click **OK**.

See also

- *Creating a Watcom SQL or Transact-SQL Function* on page 1233
- *Creating an External Java Function* on page 1235
- *Creating an External C/C++ Scalar or Aggregate Function* on page 1237
- *Deleting a Function* on page 1239
- *Generating Function DDL Commands* on page 1240
- *Granting Function EXECUTE Permission* on page 1244
- *Revoking Function EXECUTE Permission* on page 1245
- *Function Privilege Summary* on page 1246

- *Authenticating a Login Account for a Managed Resource* on page 282

Granting Function EXECUTE Permission

Grant function execute permission to users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Functions**.
3. Select a function from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Function Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
6. On the Welcome page, indicate whether the permission is being granted to a user or role.
7. Click **Next**.
8. On the Grantees page, select one or more users or roles. Click the box in the header row to select all available users or roles.
9. Click **Next**.
10. On the Permissions page, ensure **Execute** is selected.

11. Click **Finish**.

12. Click **OK**.

See also

- *Creating a Watcom SQL or Transact-SQL Function* on page 1233
- *Creating an External Java Function* on page 1235
- *Creating an External C/C++ Scalar or Aggregate Function* on page 1237
- *Deleting a Function* on page 1239
- *Generating Function DDL Commands* on page 1240
- *Viewing and Modifying a Function* on page 1241
- *Revoking Function EXECUTE Permission* on page 1245
- *Function Privilege Summary* on page 1246
- *Authenticating a Login Account for a Managed Resource* on page 282

Revoking Function EXECUTE Permission

Remove function execute permission from users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Functions**.
3. Select a function from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The Function Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, select a grantee, and click **Revoke**.
6. Click **OK**.

See also

- *Creating a Watcom SQL or Transact-SQL Function* on page 1233
- *Creating an External Java Function* on page 1235
- *Creating an External C/C++ Scalar or Aggregate Function* on page 1237
- *Deleting a Function* on page 1239
- *Generating Function DDL Commands* on page 1240
- *Viewing and Modifying a Function* on page 1241
- *Granting Function EXECUTE Permission* on page 1244
- *Function Privilege Summary* on page 1246
- *Authenticating a Login Account for a Managed Resource* on page 282

Function Privilege Summary

A list of the system privileges and object permissions required to complete the various function tasks.

Creating a Watcom SQL or Transact-SQL Function

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Watcom SQL or Transact-SQL function to be owned by self – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• RESOURCE ADMIN authority. <p>Watcom SQL or Transact-SQL function to be owned by any user –</p> <ul style="list-style-type: none">• Requires DBA authority.

Database Version	Function Privileges
SAP Sybase IQ 16.0	<p>Watcom SQL or Transact-SQL to be owned by self –</p> <ul style="list-style-type: none"> Requires CREATE PROCEDURE system privilege. <p>Watcom SQ or Transact-SQL function to be owned by any user –</p> <p>Requires one of:</p> <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege.

Creating an External C/C++ Scalar or Aggregate Function

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>External C/C++ Scalar or Aggregate function to be owned by self or any user –</p> <ul style="list-style-type: none"> Requires DBA authority.
SAP Sybase IQ 16.0	<p>External C/C++ Scalar or Aggregate function to be owned by self –</p> <p>Requires all of:</p> <ul style="list-style-type: none"> CREATE PROCEDURE system privilege. CREATE EXTERNAL REFERENCE system privilege. <p>External C/C++ Scalar or Aggregate function to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE EXTERNAL REFERENCE system privilege. Also requires one of: <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege.

Creating an External Java Function

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>External Java function to be owned by self or any user – Requires DBA authority.</p>

Database Version	Function Privileges
SAP Sybase IQ 16.0	<p>External Java function to be owned by self –</p> <p>Requires all of:</p> <ul style="list-style-type: none"> • CREATE PROCEDURE system privilege. • CREATE EXTERNAL REFERENCE system privilege. <p>External Java function to be owned by any user –</p> <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege.

Deleting a Function

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the function.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> • DROP ANY PROCEDURE system privilege. • DROP ANY OBJECT system privilege. • You own the function.

Generating Function DDL Commands

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Function Properties

Database Version	Function Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any function property page regardless of type – None required.</p> <p>Modify permissions for any function type – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object. <p>Modify any other function property regardless of type – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• You own the function.

Database Version	Function Privileges
SAP Sybase IQ 16.0	<p>View any function property page regardless of type – None required.</p> <p>Modify SQL code for Watcom SQL or Transact-SQL function – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the function. <p>Modify SQL code for External C/C++ Scalar or Aggregate, or External Java function – Requires one of:</p> <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the function. <p>Modify a comment for any function type – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • ALTER ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the function. <p>Modify permissions for any function type – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the database object.

Granting or Revoking Function EXECUTE Permission

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.

Database Version	Database Object Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You own the database object.

See also

- *Creating a Watcom SQL or Transact-SQL Function* on page 1233
- *Creating an External Java Function* on page 1235
- *Creating an External C/C++ Scalar or Aggregate Function* on page 1237
- *Deleting a Function* on page 1239
- *Generating Function DDL Commands* on page 1240
- *Viewing and Modifying a Function* on page 1241
- *Granting Function EXECUTE Permission* on page 1244
- *Revoking Function EXECUTE Permission* on page 1245

Procedures

Create, delete, display, and manage the properties of procedures in SAP Sybase IQ, including remote procedures and table-valued user-defined functions / table parameterized functions.

Sybase provides sample procedures and functions with SAP Sybase IQ. Sample procedures are visible in Sybase Control Center in the Administration Console (IQ Servers > Compiled Objects > Procedures). The samples include explanatory comments and can be found in IQ/IQ-X_X/samples/udf, where X_X is the SAP Sybase IQ release number (16.0, for example).

Creating a Procedure

Set up a new procedure on an SAP Sybase IQ server.

Prerequisites

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Watcom SQL or Transact-SQL procedure to be owned by self – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • RESOURCE ADMIN authority. <p>Watcom SQL or Transact-SQL, to be owned by any user –</p> <ul style="list-style-type: none"> • Requires DBA authority. <p>External C/C++ or External Environment procedure to be owned by self or any user – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority.
SAP Sybase IQ 16.0	<p>Watcom SQL or Transact-SQL procedure to be owned by self –</p> <ul style="list-style-type: none"> • Requires CREATE PROCEDURE system privilege. <p>Watcom SQL or Transact-SQL procedure to be owned by any user – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege <p>External C/C++ or External Environment procedure to be owned by self – Requires all of:</p> <ul style="list-style-type: none"> • CREATE EXTERNAL REFERENCE system privilege. • CREATE PROCEDURE system privilege. <p>External C/C++ or External Environment procedure to be owned by any user –</p> <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege

- The SAP Sybase IQ resource is authenticated and running.

- (Optional) If you are creating a Java procedure, install the required Java classes and JAR files in the database. (You can create the procedure if the classes and JAR files are not installed, but SAP Sybase IQ cannot execute the procedure.)
- (Optional) If you are creating a procedure that relies on a non-Java external environment, copy the library that contains the external procedure to a location accessible to the SAP Sybase IQ server. (You can create the procedure if the library is not accessible to SAP Sybase IQ, but SAP Sybase IQ cannot execute the procedure.)

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Procedures**.
3. Click the arrow next to **Procedures** and select **New**.
The Create Procedures Wizard appears.
4. On the Welcome page, specify:

Option	Description
Select a resource for which the procedure will be created	From the list, select the resource for which the procedure will be created.
Which user or group/role do you want to own the procedure?	From the list, select the user or role/group to own the procedure.
What do you want to name the procedure?	Enter a unique name for the new procedure; maximum of 128 characters.
Which SQL dialect or language do you want to use?	Select the language or SQL dialect for the procedure. If you choose External environment , click the drop-down menu to select an environment.
Use SQL template	(Optional) Select to insert a hardcoded SQL template. Leave the box unchecked to retrieve generated SQL from the back end.

5. Click **Next**.
6. On the SQL page, edit the code provided by the wizard.
 - a) For Watcom SQL and Transact-SQL, define input parameters in the format provided.
 - b) For Watcom SQL, define the result in the format provided.
 - c) For external languages, fill in the external name in the format provided.
 - d) Enter procedure statements.
 - e) Make any other changes needed to complete your procedure.
 - f) (Optional) Enter a comment describing the procedure.

Comments can include both HTML and Javadoc tags, so you can incorporate them into your generated database documentation.

7. Click **Finish**.

See also

- *Creating a Remote Procedure* on page 1254
- *Creating a Table UDF or TPF* on page 1257
- *Executing a Procedure, Table UDF, or TPF using View Data in SQL* on page 1259
- *Deleting a Procedure, Table UDF, or TPF* on page 1260
- *Generating Procedure, Table UDF, or TPF DDL Commands* on page 1261
- *Viewing or Modifying a Procedure, Table UDF, or TPF* on page 1263
- *Granting Procedure EXECUTE Permission* on page 1266
- *Revoking Procedure EXECUTE Permission* on page 1267
- *Procedure Privilege Summary* on page 1268
- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Creating an External C/C++ Scalar or Aggregate Function* on page 1237
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Remote Procedure

Define a local alias for a procedure: a means of accessing a procedure on a remote server, through a local resource. Before you can map procedures from another server to the local alias, you must define the remote server where the procedure is located.

Prerequisites

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	Remote procedure to be owned by self or any user – <ul style="list-style-type: none">• Requires DBA authority.
SAP Sybase IQ 16.0	Remote procedure to be owned by self – <ul style="list-style-type: none">• Requires CREATE PROCEDURE system privilege. Remote procedure to be owned by any user – <ul style="list-style-type: none">• Requires one of:<ul style="list-style-type: none">• CREATE ANY PROCEDURE system privilege.• CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- If the resource is a multiplex, the coordinator must be running.

Note: You must define a remote server before you can define a remote procedure on that remote server.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Procedures**.
3. Click the arrow next to **Procedures** and select **New Remote Procedure**. The Create Remote Procedures Wizard appears.
4. On the Welcome page, specify:

Option	Description
Select a resource for which the remote procedure will be created	From the list, select the resource for which the remote procedure will be created.
Which user or group/role do you want to own the remote procedure?	From the list, select the user or role/group to own the remote procedure.
Which remote server contains the procedure?	From the list, select the remote server.
Which procedure do you want to use for this remote procedure?	Select the remote procedure from the list.
What do you want to name the remote procedure?	Enter a unique name for the new remote procedure definition; maximum of 128 characters. The combination of owner and procedure name must be unique in the database

5. Click **Next**.
6. On the SQL page, edit the code provided by the wizard to provide parameter definitions for the remote procedure.

Note: When a query is made to list procedures on a remote server, the query result does not display parameters. Therefore, if a remote procedure does have set parameters (IN, OUT, IN/OUT or RESULT), they must be typed in the editor.

7. (Optional) Enter a comment to further identify the remote procedure.
8. Click **Finish**.

Example

Use a case statement to classify the results of a query:

```
CREATE PROCEDURE ProductType (IN product_id INT, OUT type CHAR(10))
BEGIN
    DECLARE prod_name CHAR(20) ;
    SELECT name INTO prod_name FROM "GROUP0"."Products"
    WHERE ID = product_id;
    CASE prod_name
        WHEN 'Tee Shirt' THEN
            SET type = 'Shirt'
        WHEN 'Sweatshirt' THEN
            SET type = 'Shirt'
        WHEN 'Baseball Cap' THEN
            SET type = 'Hat'
        WHEN 'Visor' THEN
            SET type = 'Hat'
        WHEN 'Shorts' THEN
            SET type = 'Shorts'
        ELSE
            SET type = 'UNKNOWN'
    END CASE ;
END
```

See also

- *Creating a Procedure* on page 1252
- *Creating a Table UDF or TPF* on page 1257
- *Executing a Procedure, Table UDF, or TPF using View Data in SQL* on page 1259
- *Deleting a Procedure, Table UDF, or TPF* on page 1260
- *Generating Procedure, Table UDF, or TPF DDL Commands* on page 1261
- *Viewing or Modifying a Procedure, Table UDF, or TPF* on page 1263
- *Granting Procedure EXECUTE Permission* on page 1266
- *Revoking Procedure EXECUTE Permission* on page 1267
- *Procedure Privilege Summary* on page 1268
- *Creating a Proxy Table* on page 479
- *Creating an External Login* on page 446
- *Creating a Remote Server* on page 437
- *Authenticating a Login Account for a Managed Resource* on page 282

Creating a Table UDF or TPF

Set up an external table-valued user-defined function (Table UDF) or external table parameterized function (TPF) in C/C++, or an external table-valued user-defined function in Java (Java Table UDF) on an SAP Sybase IQ server.

Prerequisites

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	<p>Table UDF or TPF to be owned by self –</p> <ul style="list-style-type: none"> Requires all of: <ul style="list-style-type: none"> CREATE EXTERNAL REFERENCE system privilege. CREATE PROCEDURE system privilege. <p>Table UDF or TPF to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE EXTERNAL REFERENCE system privilege. Also requires one of: <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- (Optional) If you are creating a Java procedure, install the required Java classes and JAR files in the database. (You can create the procedure if the classes and JAR files are not installed, but SAP Sybase IQ cannot execute the procedure.)
- (Optional) If you are creating a C/C++ procedure, copy the library that contains the procedure to a location accessible to the SAP Sybase IQ server. (You can create the procedure if the library is not accessible to SAP Sybase IQ, but SAP Sybase IQ cannot execute the procedure.)

Task

For detailed information on UDFs, in the SAP Sybase IQ documentation, see *SAP Sybase IQ User-Defined Functions*.

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Procedures**.
3. Click the arrow next to **Procedures** and select **New Table UDF/TPF**.
The Create Table UDF / TPF Wizard appears.

4. On the Welcome page, specify:

Option	Description
Select a resource for which the procedure will be created	From the list, select the resource for which the procedure will be created.
Which user or group/role do you want to own the procedure?	From the list, select the user or role/group to own the procedure.
What do you want to name the procedure?	Enter a unique name for the new procedure; maximum of 128 characters.
What do you want to create?	Select the type of table to create. Valid values are: <ul style="list-style-type: none"> • External C/C++ table UDF • External C/C++ TPF • External Java table UDF procedure from the list.
What do you want to name the remote procedure?	Enter a unique name for the new remote procedure; maximum of 128 characters.
Use SQL template	Select provide comments with syntax examples to help you define parameters and results. Leave the box unchecked if you want to use the Return Structure page to define the result.

5. Click **Next**.
6. If you chose not to use the SQL template, define the result on the Return Structure page.
7. Click **Next**.
8. On the SQL page, edit the code provided by the wizard.
 - a) Define input parameters using the format provided.
 - b) Replace the placeholder external name at the end of the query with a real name that follows the format of the placeholder.
 - c) Make any other changes needed to complete your procedure.
9. (Optional) Enter a comment describing the procedure.
Comments can include both HTML and Javadoc tags, so you can incorporate them into your generated database documentation.
10. Click **Finish**.

See also

- *Creating a Procedure* on page 1252
- *Creating a Remote Procedure* on page 1254

- *Executing a Procedure, Table UDF, or TPF using View Data in SQL* on page 1259
- *Deleting a Procedure, Table UDF, or TPF* on page 1260
- *Generating Procedure, Table UDF, or TPF DDL Commands* on page 1261
- *Viewing or Modifying a Procedure, Table UDF, or TPF* on page 1263
- *Granting Procedure EXECUTE Permission* on page 1266
- *Revoking Procedure EXECUTE Permission* on page 1267
- *Procedure Privilege Summary* on page 1268
- *Installing a Java Classes File into an SAP Sybase IQ Database* on page 1189
- *Creating an External C/C++ Scalar or Aggregate Function* on page 1237
- *Authenticating a Login Account for a Managed Resource* on page 282

Executing a Procedure, Table UDF, or TPF using View Data in SQL

Populate the Mini iSQL window with the result set of a selected procedure, remote procedure, Table UDF, or TPF.

Prerequisites

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • You have EXECUTE permission on the procedure. • You own the procedure.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • EXECUTE ANY PROCEDURE system privilege. • You have EXECUTE permission on the procedure. • You own the procedure

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Procedures**.
3. Select a procedure or remote procedure from the right pane, click the arrow to the right of the name and select **View Data in SQL**.
4. If the procedure or remote procedure has defined parameters, select a parameter to be used when executing the procedure, and select **Next**.

5. The results of the executed procedure display in SQL. Select **Execute** to execute the procedure again.

See also

- *Creating a Procedure* on page 1252
- *Creating a Remote Procedure* on page 1254
- *Creating a Table UDF or TPF* on page 1257
- *Deleting a Procedure, Table UDF, or TPF* on page 1260
- *Generating Procedure, Table UDF, or TPF DDL Commands* on page 1261
- *Viewing or Modifying a Procedure, Table UDF, or TPF* on page 1263
- *Granting Procedure EXECUTE Permission* on page 1266
- *Revoking Procedure EXECUTE Permission* on page 1267
- *Procedure Privilege Summary* on page 1268
- *Creating an External Login* on page 446
- *Creating a Proxy Table* on page 479
- *Creating a Remote Server* on page 437
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Procedure, Table UDF, or TPF

Remove a procedure, remote procedure, Table UDF, or TPF from an SAP Sybase IQ server.

Prerequisites

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• You own the procedure.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• DROP ANY PROCEDURE system privilege.• DROP ANY OBJECT system privilege.• You own the procedure.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Compiled Objects > Procedures**.
3. Select one or more procedures, remote procedures, Table UDFs or TPFs from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or
 - From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple procedures.

4. Click **Yes** to confirm the deletion.

See also

- *Creating a Procedure* on page 1252
- *Creating a Remote Procedure* on page 1254
- *Creating a Table UDF or TPF* on page 1257
- *Executing a Procedure, Table UDF, or TPF using View Data in SQL* on page 1259
- *Generating Procedure, Table UDF, or TPF DDL Commands* on page 1261
- *Viewing or Modifying a Procedure, Table UDF, or TPF* on page 1263
- *Granting Procedure EXECUTE Permission* on page 1266
- *Revoking Procedure EXECUTE Permission* on page 1267
- *Procedure Privilege Summary* on page 1268
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Procedure, Table UDF, or TPF DDL Commands

Generate the data description language for creating a procedure, remote procedure, Table UDF, or TPF on an SAP Sybase IQ server. The DDL code can be a useful reference and training tool.

Prerequisites

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.

2. In the left pane, select **IQ Servers > Compiled Objects > Procedures**.
3. Select one or more procedures, remote procedures, Table UDFs, or TPFs from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple procedures.

The DDL view shows the SQL code used to add the selected procedures.

See also

- *Creating a Procedure* on page 1252
- *Creating a Remote Procedure* on page 1254
- *Creating a Table UDF or TPF* on page 1257
- *Executing a Procedure, Table UDF, or TPF using View Data in SQL* on page 1259
- *Deleting a Procedure, Table UDF, or TPF* on page 1260
- *Viewing or Modifying a Procedure, Table UDF, or TPF* on page 1263
- *Granting Procedure EXECUTE Permission* on page 1266
- *Revoking Procedure EXECUTE Permission* on page 1267
- *Procedure Privilege Summary* on page 1268
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying a Procedure, Table UDF, or TPF

Examine the SQL statement and properties of a procedure, remote procedure, Table UDF, or TPF on an SAP Sybase IQ server. You can edit the SQL statement and change some property values.

Prerequisites

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any procedure property page regardless of type – None required.</p> <p>Modify permissions for any procedure type – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object. <p>Modify any other procedure property regardless of type – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• You own the procedure.

Database Version	Procedure Privileges
SAP Sybase IQ 16.0	<p>View any procedure property page regardless of type – None required.</p> <p>Modify SQL code for Watcom-SQL or Transcat-SQL procedures – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the procedure. <p>Modify SQL code for Table UDFs, TPFs, or External Environment procedures –</p> <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the procedure. <p>Modify a comment for any procedure type – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • ALTER ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the procedure. <p>Modify permissions for any procedure type – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Procedures**.
3. Select a procedure from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Procedure Properties view appears.

4. View or modify the properties.

- When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
- If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) The name of the procedure.</p> <p>Owner – (Read-only) The owner of the procedure.</p> <p>Creation Time – (Read-only) The date and time the procedure was created.</p> <p>Dialect – (Read-only) The dialect of the procedure. Valid values are:</p> <ul style="list-style-type: none"> • Watcom-SQL • Transact-SQL • External C/C++ scalar • External C/C++ aggregate • External Java <p>Comment – A text field for adding an optional comment about the procedure.</p>
Parameters (Read-only)	The parameters defined from the procedure.
SQL	The SQL code to be executed by the procedure.
Permissions	See <i>Granting Procedure EXECUTE Permission</i> on page 1266 and <i>Revoking Procedure EXECUTE Permission</i> on page 1267.

5. Click **OK**.

See also

- *Creating a Procedure* on page 1252
- *Creating a Remote Procedure* on page 1254
- *Creating a Table UDF or TPF* on page 1257
- *Executing a Procedure, Table UDF, or TPF using View Data in SQL* on page 1259
- *Deleting a Procedure, Table UDF, or TPF* on page 1260
- *Generating Procedure, Table UDF, or TPF DDL Commands* on page 1261
- *Granting Procedure EXECUTE Permission* on page 1266
- *Revoking Procedure EXECUTE Permission* on page 1267

- *Procedure Privilege Summary* on page 1268
- *Authenticating a Login Account for a Managed Resource* on page 282

Granting Procedure EXECUTE Permission

Grant procedure execute permission to users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none">• DBA authority.• PERMS ADMIN authority.• You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none">• MANAGE ANY OBJECT PRIVILEGE system privilege.• You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Procedures**.
3. Select a procedure from the right pane and either:
 - Click the arrow to the right of the name and select **Properties**, or
 - From the Administration Console menu bar, select **Resource > Properties**.

The Procedure Properties view appears.

4. In the left pane, click **Permissions**.
5. In the right pane, click **Grant**.
The Grant Permission Wizard appears.
6. On the Welcome page, indicate whether the permission is being granted to a user or role.
7. Click **Next**.
8. On the Grantees page, select one or more users or roles. Click the box in the header row to select all available users or roles.
9. Click **Next**.

10. On the Permissions page, ensure **Execute** is selected.

11. Click **Finish**.

12. Click **OK**.

See also

- *Creating a Procedure* on page 1252
- *Creating a Remote Procedure* on page 1254
- *Creating a Table UDF or TPF* on page 1257
- *Executing a Procedure, Table UDF, or TPF using View Data in SQL* on page 1259
- *Deleting a Procedure, Table UDF, or TPF* on page 1260
- *Generating Procedure, Table UDF, or TPF DDL Commands* on page 1261
- *Viewing or Modifying a Procedure, Table UDF, or TPF* on page 1263
- *Revoking Procedure EXECUTE Permission* on page 1267
- *Procedure Privilege Summary* on page 1268
- *Authenticating a Login Account for a Managed Resource* on page 282

Revoking Procedure EXECUTE Permission

Remove procedure execute permission from users and roles.

Prerequisites

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	Requires one of: <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the database object.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

1. In the Perspective Resources view, select the resource and select **Resource > Administration Console**.
2. In the Administration Console, expand **IQ Servers > Compiled Objects > Procedures**.

3. Select a procedure from the right pane and either:

- Click the arrow to the right of the name and select **Properties**, or
- From the Administration Console menu bar, select **Resource > Properties**.

The Procedure Properties view appears.

4. In the right pane, select a grantee, and click **Revoke**.

5. Click **OK**.

See also

- *Creating a Procedure* on page 1252
- *Creating a Remote Procedure* on page 1254
- *Creating a Table UDF or TPF* on page 1257
- *Executing a Procedure, Table UDF, or TPF using View Data in SQL* on page 1259
- *Deleting a Procedure, Table UDF, or TPF* on page 1260
- *Generating Procedure, Table UDF, or TPF DDL Commands* on page 1261
- *Viewing or Modifying a Procedure, Table UDF, or TPF* on page 1263
- *Granting Procedure EXECUTE Permission* on page 1266
- *Procedure Privilege Summary* on page 1268
- *Authenticating a Login Account for a Managed Resource* on page 282

Procedure Privilege Summary

A list of the system privileges and object permissions required to complete the various procedure tasks.

Creating a Procedure

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Watcom SQL or Transact-SQL procedure to be owned by self – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.• RESOURCE ADMIN authority. <p>Watcom SQL or Transact-SQL, to be owned by any user –</p> <ul style="list-style-type: none">• Requires DBA authority. <p>External C/C++ or External Environment procedure to be owned by self or any user – Requires one of:</p> <ul style="list-style-type: none">• DBA authority.

Database Version	Procedure Privileges
SAP Sybase IQ 16.0	<p>Watcom SQL or Transact-SQL procedure to be owned by self –</p> <ul style="list-style-type: none"> Requires CREATE PROCEDURE system privilege. <p>Watcom SQL or Transact-SQL procedure to be owned by any user – Requires one of:</p> <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege <p>External C/C++ or External Environment procedure to be owned by self – Requires all of:</p> <ul style="list-style-type: none"> CREATE EXTERNAL REFERENCE system privilege. CREATE PROCEDURE system privilege. <p>External C/C++ or External Environment procedure to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE EXTERNAL REFERENCE system privilege. Also requires one of: <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege

Creating a Remote Procedure

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Remote procedure to be owned by self or any user –</p> <ul style="list-style-type: none"> Requires DBA authority.
SAP Sybase IQ 16.0	<p>Remote procedure to be owned by self –</p> <ul style="list-style-type: none"> Requires CREATE PROCEDURE system privilege. <p>Remote procedure to be owned by any user –</p> <ul style="list-style-type: none"> Requires one of: <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege.

Creating a Table UDF or TPF

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	<p>Table UDF or TPF to be owned by self –</p> <ul style="list-style-type: none"> Requires all of: <ul style="list-style-type: none"> CREATE EXTERNAL REFERENCE system privilege. CREATE PROCEDURE system privilege. <p>Table UDF or TPF to be owned by any user –</p> <ul style="list-style-type: none"> Requires CREATE EXTERNAL REFERENCE system privilege. Also requires one of: <ul style="list-style-type: none"> CREATE ANY PROCEDURE system privilege. CREATE ANY OBJECT system privilege.

Executing a Procedure Using View Data in SQL

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> DBA authority. You have EXECUTE permission on the procedure. You own the procedure.
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> EXECUTE ANY PROCEDURE system privilege. You have EXECUTE permission on the procedure. You own the procedure

Deleting a Procedure

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> DBA authority. You own the procedure.

Database Version	Procedure Privileges
SAP Sybase IQ 16.0	Requires one of: <ul style="list-style-type: none"> • DROP ANY PROCEDURE system privilege. • DROP ANY OBJECT system privilege. • You own the procedure.

Generating Procedure DDL Commands

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Procedure Properties

Database Version	Procedure Privileges
SAP Sybase IQ 15.3 and 15.4	<p>View any procedure property page regardless of type – None required.</p> <p>Modify permissions for any procedure type – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object. <p>Modify any other procedure property regardless of type – Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • You own the procedure.

Database Version	Procedure Privileges
SAP Sybase IQ 16.0	<p>View any procedure property page regardless of type – None required.</p> <p>Modify SQL code for Watcom-SQL or Transcat-SQL procedures – Requires one of:</p> <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the procedure. <p>Modify SQL code for Table UDFs, TPFs, or External Environment procedures –</p> <ul style="list-style-type: none"> • Requires CREATE EXTERNAL REFERENCE system privilege. • Also requires one of: <ul style="list-style-type: none"> • ALTER ANY PROCEDURE system privilege. • ALTER ANY OBJECT system privilege. • You own the procedure. <p>Modify a comment for any procedure type – Requires one of:</p> <ul style="list-style-type: none"> • CREATE ANY PROCEDURE system privilege. • ALTER ANY PROCEDURE system privilege. • CREATE ANY OBJECT system privilege. • ALTER ANY OBJECT system privilege. • COMMENT ANY OBJECT system privilege. • You own the procedure. <p>Modify permissions for any procedure type – Requires one of:</p> <ul style="list-style-type: none"> • MANAGE ANY OBJECT PRIVILEGE system privilege. • You own the database object.

Granting or Revoking Procedure EXECUTE Permission

Database Version	Database Object Privileges
SAP Sybase IQ 15.3 and 15.4	<p>Requires one of:</p> <ul style="list-style-type: none"> • DBA authority. • PERMS ADMIN authority. • You own the database object.

Database Version	Database Object Privileges
SAP Sybase IQ 16.0	<p>Requires one of:</p> <ul style="list-style-type: none"> MANAGE ANY OBJECT PRIVILEGE system privilege. You own the database object.

See also

- *Creating a Procedure* on page 1252
- *Creating a Remote Procedure* on page 1254
- *Creating a Table UDF or TPF* on page 1257
- *Executing a Procedure, Table UDF, or TPF using View Data in SQL* on page 1259
- *Deleting a Procedure, Table UDF, or TPF* on page 1260
- *Generating Procedure, Table UDF, or TPF DDL Commands* on page 1261
- *Viewing or Modifying a Procedure, Table UDF, or TPF* on page 1263
- *Granting Procedure EXECUTE Permission* on page 1266
- *Revoking Procedure EXECUTE Permission* on page 1267

Web Services

The system store (IQ catalog store) contains a built-in HTTP server that allows you to provide Web services, as well as to access Web services in other databases and over the Internet. You can manage Web services only for system store tables.

Web services define valid URLs and their functionality. Web services commonly facilitate data transfer and interoperability. You create and store Web services in databases; a single database can define multiple Web services. You can define Web services in different databases so that they appear to be part of a single Web site.

Simple Object Access Protocol (SOAP) is the standard used for access, but the built-in HTTP server also lets you handle standard HTTP and HTTPS requests from client applications.

SOAP provides a method for internet communication, between applications such as those written in Java, or a Microsoft .NET language like Visual C#. SOAP messages define the services that a server provides. Actual data transfer generally takes place using HTTP. Any application, such as a client or server, that participates in SOAP communication is called a SOAP node or SOAP endpoint. Such applications can transmit, receive, or process SOAP messages.

SAP Sybase IQ Web services can listen for and handle standard SOAP requests. Web services provide client applications an alternative to such traditional interfaces as JDBC and ODBC. Web services can be accessed from client applications written in a variety of languages and running on a variety of platforms. Even common scripting languages such as Perl and Python

provide access to Web services. You create Web services in a database using the **CREATE SERVICE** statement.

SAP Sybase IQ can also function as a SOAP or HTTP client, permitting applications running within the database to access standard Web services available over the Internet, or provided by other SAP Sybase IQ databases. This client functionality is accessed through stored functions and procedures.

In addition, the term Web services also refers to applications that use the built-in Web server to handle HTTP requests from clients. These applications generally function like traditional database-backed Web applications, but can be more compact and are easier to write as the data and the entire application can reside within a database. In this type of application, the Web service typically returns documents in HTML format. The GET, HEAD, and POST methods are supported.

The collection of Web services within your database together define the available URLs. Each service provides a set of Web pages. Typically, the content of these pages is generated by procedures that you write and store in your database, although they can be a single statement or, optionally, allow users to execute statements of their own. These Web services become available when you start the database server with options that enable it to listen for HTTP requests.

Since the HTTP server that handles Web service requests is embedded in the database, performance is good. Applications that use Web services are easily deployed, since no additional components are needed, beyond the database and database server.

Creating a Web Service

Create a Web service to facilitate data transfer with SOAP or HTTP.

Prerequisites

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY WEB SERVICE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

Web service definitions are stored in the system store (catalog store) only.

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Web Services**.

3. Click the arrow next to **Web Services** and select **New**.
The Create Web Service Wizard appears.
4. On the Welcome page, specify:

Option	Description
Select a resource for which the web service will be created	From the list, select the resource for which the Web service will be created.
(Multiplex only) Select a multiplex server on which the web service will be created?	From the list, select the multiplex server on which the Web service will be created.
SCC agent status	The SCC agent for the multiplex server must be registered and authenticated in order to create a Web service on it. If the SCC Agent status indicates unregistered, click the Register Agent and Authenticate Agent buttons to register and authenticate.
What do you want to name the new web service?	Enter a unique name for the new procedure; maximum of 128 characters. The Web service name must not begin or end with a slash (/) or contain two or more consecutive slashes.

5. Click **Next**.
6. On the Type page, specify:

Option	Description
Which type of web service do you want to create?	<p>From the list, select the Web service type. Valid values are:</p> <ul style="list-style-type: none"> • Raw – the result set of the SQL statement or procedure is sent to the client without any additional formatting. You must enable authorization if this service does not have a statement. • XML – the result set of the SQL statement or procedure is assumed to be XML; if it is not, then the result set is converted to XML RAW format. You must enable authorization if this service does not have a statement. • HTML – the result set of the SQL statement or procedure is formatted as an HTML document with a table containing the rows and columns. You must enable authorization if this service does not have a statement. • JSON – the result set of the SQL statement or procedure is formatted as JSON (JavaScript Object Notation) serialized data represented as an array of row structures containing column and value pairs. You must enable authorization if this service does not have a statement. • SOAP – the request must be a valid SOAP (Simple Object Access Protocol) request, and the result set is formatted as a SOAP response. • DISH – a DISH service acts as a proxy for a group of SOAP services and generates a WSDL (Web Services Description Language) file for each of its SOAP services.
Do you want this web service to be enabled.	Select to enable the Web service.

7. Click **Next**.

8. (For Raw, XML, HTML or JSON service types only) On the URL Path page, specify whether the remainder of the URL path is permitted, and if so, how it is processed. Valid values are:

Option	Description
Off	The remainder of the URL path is not permitted. e.g. http://<host-name>/<service-name>
On	The remainder of the URL path is permitted and is set as a single parameter. e.g. http://<host-name>/<service-name>/aaa/bbb/cc url=aaa/bbb/cc

Option	Description
Elements	The remainder of the URL path is permitted and is set as multiple parameters. e.g. http://<host-name>/<service-name>/aaa/bbb/ccc url1=aaa, url2=bbb, url3=ccc

9. Click **Next**.

10. For SOAP or DISH service types only) On the Data Payload Format page, specify type of data payload format the Web service should expose. Valid values are:

Format	Description
Default	This format is equivalent to .NET in all cases except for SOAP services that are handled by a DISH service. In such cases, the DISH service's format is used instead of the SOAP service's format.
.NET	This format is used for .NET clients that can accept Microsoft's Dataset format. This is useful to SOAP clients developed with Microsoft and Microsoft-compatible tools.
Concrete	This is a generic format used by SOAP toolkits such as JAX-RPC (JAVA) to generate interfaces that correlate to a result set returned by SQL Anywhere. Select Expose an explicit response object for this web service to have this web service expose an explicit response object if the service calls a procedure that returns a result set. The XML schema of this object will contain column names and data types based on the result set.
XML	This is the most compatible format; it simply returns the result set as a string. Clients will need to parse this string to access the various elements within it.

11. Click **Next**.

12. For SOAP service type only) On the Data Type Behavior page, specify which data typing behavior to be used for this Web service. Valid formats are:

Behavior	Description
Off	This is the default behavior. No data typing of inputs and outputs (DNET is String only). Equivalent to the behavior in SQL Anywhere version 9.0.x.
On	Supports data typing for input parameters and result set responses.
In	Supports data typing for input parameters only. XML and CONCRETE formats contain no type information; DNET is String only.

Behavior	Description
Out	Supports data typing for result set responses of all SOAP service formats; input parameters are Strings only.

13. Click **Next**.

14. (For DISH service type only) (Optional) On the Service Name Prefix page, specify a SOAP service name prefix to specify the group of SOAP services that apply to this DISH service. Only those SOAP services whose names begin with this prefix will be handled by this DISH service.

15. Click **Next**.

16. On the Methods page, specify the request methods to be enabled for the Web service. Valid methods are:

Available methods depend on the service type specified.

Method	Description
HEAD	Retrieve information written in a response header.
GET	Request a response
POST	Submit data to be processed by a resource
PUT	Upload a resource
DELETE	Remove a resource

17. Click **Next**.

18. On the Authorization page specify:

Option	Description
Require authentication for this web service	Select if authentication is required to execute the Web service.
User	If user authentication is required, select a user from the list.

19. Click **Next**.

20. On the Security page, select the option to configure the Web service to only be processed if the request is made through a secure (HTTPS) connection. If a request to a secure web service is received on the HTTP port, then the request will be redirected to the HTTPS port.

21. Click **Next**.

22. On the SQL Statement page, specify a SQL command, (usually a stored procedure) called when someone accesses a service.

Defining an SQL command is optional for Raw, XML, HTML or JSON service types. You must select the **This web service has the following SQL statement** option before you can

enter the SQL command. For SOAP or DISH service types, the **This web service has the following SQL statement** option is unavailable since defining an SQL command is mandatory.

Services without statements cause serious security risk because they permit Web clients to execute arbitrary commands. When creating services without statements, you must enable authorization, which forces all clients to provide a valid user name and password. Sybase recommends that all production systems define statements in their services.

In a non-production environment, you can create services that do not include statements. Services configured in this way can be useful when you are testing a service, or want a general way to access information. Either omit the statement entirely or use the phrase **NULL** in place of the statement.

23. Click **Next**.

24. (Optional) On the Comment page, specify a comment for the Web service.

25. Click **Finish**.

See also

- *Enabling a Web Service* on page 1279
- *Disabling a Web Service* on page 1280
- *Deleting a Web Service* on page 1281
- *Generating Web Service DDL Commands* on page 1282
- *Viewing or Modifying Web Services Properties* on page 1283
- *Web Service Privilege Summary* on page 1286
- *Authenticating a Login Account for a Managed Resource* on page 282

Enabling a Web Service

Enable a disabled Web service so the service can listen for requests over HTTP or HTTPS.

Prerequisites

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY WEB SERVICE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The Web service is disabled.

Task

Web service definitions are stored in the system store (catalog store) only.

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Web Services**.
3. Select one or more Web services from the right pane and either:
 - Click the arrow to the right of the name and select **Enabled**, or
 - From the Administration Console menu bar, select **Resource > Enabled**.

Tip: Use **Shift-click** or **Control-click** to select multiple Web services.

Note: A disabled Web service has a value of `false` in the **Enabled** column.

4. Click **Yes** to confirm enabling.

See also

- *Creating a Web Service* on page 1274
- *Disabling a Web Service* on page 1280
- *Deleting a Web Service* on page 1281
- *Generating Web Service DDL Commands* on page 1282
- *Viewing or Modifying Web Services Properties* on page 1283
- *Web Service Privilege Summary* on page 1286
- *Authenticating a Login Account for a Managed Resource* on page 282

Disabling a Web Service

Disable a Web service to prevent the service from listening for requests over HTTP or HTTPS. The Web service definition remains in the database.

Prerequisites

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires <code>MANAGE ANY WEB SERVICE</code> system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.
- The Web service is enabled.

Task

Web service definitions are stored in the system store (catalog store) only.

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Web Services**.

3. Select one or more Web services from the right pane and either:
 - Click the arrow to the right of the name and select **Disable**, or
 - From the Administration Console menu bar, select **Resource > Disable**.

Tip: Use **Shift-click** or **Control-click** to select multiple Web services.

Note: An enabled Web service has a value of `true` in the **Enabled** column.

4. Click **Yes** to confirm disabling.

See also

- *Creating a Web Service* on page 1274
- *Enabling a Web Service* on page 1279
- *Deleting a Web Service* on page 1281
- *Generating Web Service DDL Commands* on page 1282
- *Viewing or Modifying Web Services Properties* on page 1283
- *Web Service Privilege Summary* on page 1286
- *Authenticating a Login Account for a Managed Resource* on page 282

Deleting a Web Service

Delete an enabled or disabled Web service to permanently remove the object and its definition from the server.

Prerequisites

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY WEB SERVICE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- In a multiplex configuration, the coordinator node is running.

Task

Web service definitions are stored in the system store (catalog store) only.

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Web Services**.
3. Select one or more Web services from the right pane and either:
 - Click the arrow to the right of the name and select **Delete**, or

- From the Administration Console menu bar, select **Resource > Delete**.

Tip: Use **Shift-click** or **Control-click** to select multiple Web services.

4. Click **Yes** to confirm deletion.

See also

- *Creating a Web Service* on page 1274
- *Enabling a Web Service* on page 1279
- *Disabling a Web Service* on page 1280
- *Generating Web Service DDL Commands* on page 1282
- *Viewing or Modifying Web Services Properties* on page 1283
- *Web Service Privilege Summary* on page 1286
- *Authenticating a Login Account for a Managed Resource* on page 282

Generating Web Service DDL Commands

Display the data description language SQL code for adding a Web service to the catalog store. The SQL code can be a useful reference and training tool.

Prerequisites

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

- The SAP Sybase IQ resource is authenticated and running.

Task

Web service definitions are stored in the system store (catalog store) only.

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Web Services**.
3. Select one or more Web services from the right pane and either:
 - Click the arrow to the right of the name and select **Generate DDL**, or
 - From the Administration Console menu bar, select **Resource > Generate DDL**.

Tip: Use **Shift-click** or **Control-click** to select multiple Web services.

The DDL view shows the SQL code used to add the selected Web service to the catalog store.

See also

- *Creating a Web Service* on page 1274
- *Enabling a Web Service* on page 1279
- *Disabling a Web Service* on page 1280
- *Deleting a Web Service* on page 1281
- *Viewing or Modifying Web Services Properties* on page 1283
- *Web Service Privilege Summary* on page 1286
- *Authenticating a Login Account for a Managed Resource* on page 282

Viewing or Modifying Web Services Properties

Display or change the properties of the selected Web service.

Prerequisites

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	View any Web service property page – None required. Modify any Web service property – Requires DBA authority.
SAP Sybase IQ 16.0	View any Web service property page – None required. Modify any Web service property – Requires MANAGE ANY WEB SERVICE system privilege.

- The SAP Sybase IQ resource is authenticated and running.
- (Modifying properties only) In a multiplex configuration, the coordinator node is running.

Task

1. From the application menu bar, select **View > Open > Administration Console**.
2. In the left pane, select **IQ Servers > Compiled Objects > Web Services**.
3. Select a Web service in the right pane, click the drop-down arrow that appears to the right, and select **Properties**.
4. View or modify Web service properties.
 - When modifying properties, clicking **Apply** before changing screens is not necessary, but will save any changes.
 - If you do not have privileges to modify properties, Sybase Control Center displays the properties view in read-only mode.

Area	Description
General	<p>Name – (Read-only) Shows the name of the selected web service.</p> <p>Enabled – Select this option to enable the web service to listen for requests over HTTP or HTTPS. By default, database servers do not listen for web service requests, leaving no way for clients to access any services that may be defined in your database. If you clear this option, the database server keeps the definition of the web service in the database, but makes the web service unusable.</p> <p>Service type – Shows whether the selected web service is a RAW, XML, HTML, JSON, SOAP, or DISH web service. You can change the service type by choosing a different type from the dropdown list.</p> <p>URL path – Specifies whether URL paths are accepted, and if so, how they are processed. The options are:</p> <ul style="list-style-type: none"> • Off – Select this option if the remainder of the URL path is not permitted. If the service name ends with a forward slash (/), select Off. For example, if Off is selected and you have the URL path <code>http://<host-name>/<service-name>/aaa/bbb/ccc</code>, only <code>http://<host-name>/<service-name></code> is permitted. The remainder of the URL path, <code>/aaa/bbb/ccc</code> is not permitted. • On – Select this option if the remainder of the URL path is permitted and is set as a single parameter. For example, in the URL path <code>http://<host-name>/<service-name>/aaa/bbb/ccc</code>, the remainder of the URL path is <code>/aaa/bbb/ccc</code>. It is treated as a single parameter. • Elements – Select this option if the remainder of the URL path is permitted and is set as multiple parameters. For example, in the URL path <code>http://<host-name>/<service-name>/aaa/bbb/ccc</code>, each element of the path is treated as a separate parameter. For example, <code>url1=aaa</code>, <code>url2=bbb</code>, <code>url3=ccc</code>, and so on. <p>Format – (SOAP and DISH services only.) Generates output formats compatible with various types of SOAP clients, such as .NET or Java JAX-RPC. If a SOAP service's format is not specified, the format is inherited from the service's DISH service declaration. If the DISH service does not declare a format, it defaults to DNET, which is compatible with .NET clients. A SOAP service that does not declare a format can be used with different types of SOAP clients by defining multiple DISH services, each with a different format type.</p> <ul style="list-style-type: none"> • Expose an explicit response object – This option only affects the WSDL document that is generated. Select this option to have the DISH service return an XML schema that explicitly describes the result set. It returns all

Area	Description
	<p>the column names and their data types in the result set. If you don't select this option, then the DISH service returns an XML schema (a WSDL document) that describes the generic SimpleDataset object. The SimpleDataset describes a rowset consisting of rows and columns; no column name or data type information is returned.</p> <p>Data type – (SOAP services only.) SOAP service data typing:</p> <ul style="list-style-type: none"> • OFF – (Default) No data typing of inputs and outputs. • ON – Supports data typing of input parameters and result set responses. • IN – Supports data typing of input parameters only. • OUT – Provides data type information for result set responses of all SOAP service formats. <p>Service name prefix – (DISH services only.) Only SOAP services whose names begin with this prefix are handled by the DISH service.</p> <p>Methods – Select one or more of the following request methods: HEAD, GET, POST, PUT, or DELETE.</p> <p>Authorization required – Indicates whether users must authenticate to use this web service. When authorization is required, all users connecting to this service must provide a user name and password. If you select the User check box, you must authenticate as the specified user to use this web service. However, if User is cleared and authentication is required, then you can authenticate with any database user to use this web service. If authorization is not required, you must choose a user from the dropdown list . All requests are run using the account and permissions of the user specified.</p> <ul style="list-style-type: none"> • User – Shows which user account is used to execute service requests. If the service does not require authorization, you must choose a user from the dropdown list. • Security required – Shows whether unsecured connections are accepted. Select this option to indicate that the web service requires security. If the web service requires security, then only secure (HTTPS) connections are accepted. If this option is cleared, then both HTTP and HTTPS connections are accepted. <p>Comment – Text description of the Web service. For example, describe the Web service's purpose in the system.</p>
SQL	<p>This web service has the following SQL statement – Enables the text box where you can specify the SQL statement for the Web service.</p> <p>SQL statement area – Text box containing the SQL statement for the Web service.</p>

5. Click **OK**.

See also

- *Creating a Web Service* on page 1274
- *Enabling a Web Service* on page 1279
- *Disabling a Web Service* on page 1280
- *Deleting a Web Service* on page 1281
- *Generating Web Service DDL Commands* on page 1282
- *Web Service Privilege Summary* on page 1286
- *Authenticating a Login Account for a Managed Resource* on page 282

Web Service Privilege Summary

A list of the system privileges and object permissions required to complete the various Web service tasks.

Creating a Web Service

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY WEB SERVICE system privilege.

Enabling or Disabling a Web Service

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY WEB SERVICE system privilege.

Deleting a Web Service

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	Requires DBA authority.
SAP Sybase IQ 16.0	Requires MANAGE ANY WEB SERVICE system privilege.

Generating Web Service DDL Commands

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	None required.
SAP Sybase IQ 16.0	None required.

Viewing or Modifying Web Service Properties

Database Version	Web Service Privileges
SAP Sybase IQ 15.3 and 15.4	View any Web service property page – None required. Modify any Web service property – Requires DBA authority.
SAP Sybase IQ 16.0	View any Web service property page – None required. Modify any Web service property – Requires MANAGE ANY WEB SERVICE system privilege.

See also

- *Creating a Web Service* on page 1274
- *Enabling a Web Service* on page 1279
- *Disabling a Web Service* on page 1280
- *Deleting a Web Service* on page 1281
- *Generating Web Service DDL Commands* on page 1282
- *Viewing or Modifying Web Services Properties* on page 1283

Manage Sybase Control Center

All Sybase products using Sybase Control Center share high-level management features, including the Administration Console, data collection jobs, alerts, logs, resources, perspectives, and views.

Use these management features to perform high-level management tasks. These tasks apply to any Sybase product you manage with Sybase Control Center.

Job Scheduling

A schedule defines a data collection job and specifies how often the job executes in your system.

In Sybase Control Center, collection jobs provide the data that appears on monitoring screens and charts. A collection is a set of key performance indicators (KPIs). When the scheduler runs a collection job, it gathers the value of each KPI in the collection and tags the data with the date and time it was gathered. The data is stored in the repository and displayed. Each product module has predefined collections that you can schedule.

You can define schedules as one-time or repeating. You can modify the schedule for a job based on a number of attributes such as:

- Repeat interval
- Date
- Time

The job history displays the status of jobs executed each day.

See also

- *Setting Up Statistics Collection* on page 283
- *SAP Sybase IQ Data Collections* on page 286

Executing and Stopping a Data Collection Job

Use the Properties view to execute or stop a data collection job.

Most of the time, data collection jobs should run on a schedule; you should rarely need to start or stop a job manually.

1. In the Perspective Resources view, select the resource associated with the job and select **Resource > Properties**.
2. Select **Collection Jobs**.

3. Select the job and:

- To execute a job immediately, click **Execute**.
- To stop a job, click **Stop**, then click **Yes** to confirm.

See also

- *Deleting a Data Collection Job* on page 1290
- *Resuming and Suspending a Data Collection Job* on page 1290
- *Adding a New Schedule to a Job* on page 1291
- *Viewing or Deleting a Schedule* on page 1292
- *Modifying the Data Collection Interval for a Job* on page 1293
- *Resuming and Suspending the Scheduler* on page 1293
- *Viewing the Job Execution History* on page 1294

Deleting a Data Collection Job

Use the Properties view for a resource to delete one or more data collection jobs.

1. In the Perspective Resources view, select the resource associated with the job and select **Resource > Properties**.
2. Select **Collection Jobs**.
3. Select the job and click **Delete**.
4. Click **OK** to confirm the deletion.

See also

- *Executing and Stopping a Data Collection Job* on page 1289
- *Resuming and Suspending a Data Collection Job* on page 1290
- *Adding a New Schedule to a Job* on page 1291
- *Viewing or Deleting a Schedule* on page 1292
- *Modifying the Data Collection Interval for a Job* on page 1293
- *Resuming and Suspending the Scheduler* on page 1293
- *Viewing the Job Execution History* on page 1294

Resuming and Suspending a Data Collection Job

Use the Properties view for a resource to resume or suspend a data collection job.

1. In the Perspective Resources view, select the resource associated with the job and select **Resource > Properties**.
2. Select **Collection Jobs**.
3. Select the job (a top-level item in the Collection Jobs table). On the **General** tab:

- To resume a job, click **Resume**.
- To suspend a job, click **Suspend**, then click **Yes** to confirm the suspension.

Tip: If the **General** tab is grayed out, you have selected a schedule (child) rather than a job (parent) in the Collection Jobs table. Select the parent job to display the **General** tab.

See also

- *Executing and Stopping a Data Collection Job* on page 1289
- *Deleting a Data Collection Job* on page 1290
- *Adding a New Schedule to a Job* on page 1291
- *Viewing or Deleting a Schedule* on page 1292
- *Modifying the Data Collection Interval for a Job* on page 1293
- *Resuming and Suspending the Scheduler* on page 1293
- *Viewing the Job Execution History* on page 1294

Adding a New Schedule to a Job

Use the Properties view for a resource to add schedules to a data collection job.

1. In the Perspective Resources view, select the resource associated with the job and select **Resource > Properties**.
2. Select **Collection Jobs**.
3. Select the job.
4. Click **Add Schedule**.
5. Specify details for the new schedule:

Field	Description
Name	A name for this schedule
Description	A description of this schedule

6. Choose to start the job **Now** or **Later**. If you choose **Later**, specify the start date and time.
7. Specify the duration of this schedule. The job can run:

- **Once**
- **Repetitively** at an interval you specify

Field	Description
Repeat interval	Time period (in seconds, minutes, hours, or days) between job executions

- **Until** a stop date that you specify, at an interval you specify

Field	Description
Repeat interval	Time period (in seconds, minutes, hours, or days) between job executions
Stop date	Date and time the job should stop running

Note: Enter dates and times using your local time. Sybase Control Center converts your times for remote time zones if necessary.

You cannot change the duration of a schedule (the once/repetitively/until setting) after you create it. To change the schedule duration, delete and recreate the schedule.

8. Click **Finish** to save the schedule.
9. Click **OK**.

See also

- *Executing and Stopping a Data Collection Job* on page 1289
- *Deleting a Data Collection Job* on page 1290
- *Resuming and Suspending a Data Collection Job* on page 1290
- *Viewing or Deleting a Schedule* on page 1292
- *Modifying the Data Collection Interval for a Job* on page 1293
- *Resuming and Suspending the Scheduler* on page 1293
- *Viewing the Job Execution History* on page 1294

Viewing or Deleting a Schedule

Display schedule details or remove a schedule from a data collection job.

1. In the Perspective Resources view, select the resource associated with the job and select **Resource > Properties**.
2. Select **Collection Jobs**.
3. To display the schedules for a collection job, expand the job by clicking the arrow to the left of the job's name.
If there is no arrow to the left of the job's name, this job has no schedules.
4. Select a schedule.
The name, description, start and end dates, and repeat interval appear on the Schedule tab.
5. (Optional) To remove the selected schedule, click **Delete**.
6. Click **OK**.

See also

- *Executing and Stopping a Data Collection Job* on page 1289
- *Deleting a Data Collection Job* on page 1290
- *Resuming and Suspending a Data Collection Job* on page 1290
- *Adding a New Schedule to a Job* on page 1291
- *Modifying the Data Collection Interval for a Job* on page 1293
- *Resuming and Suspending the Scheduler* on page 1293
- *Viewing the Job Execution History* on page 1294
- *Setting Up Statistics Collection* on page 283

Modifying the Data Collection Interval for a Job

Use the Properties view for a managed resource to modify the data collection schedule.

1. In the Perspective Resources view, select a server (or other resource).
2. In the view's menu bar, select **Resource > Properties**.
3. Select **Collection Jobs**.
4. Expand a job folder and select a schedule.
5. On the **Schedule** tab, modify the Repeat interval field.
6. Click **Apply**.

See also

- *Executing and Stopping a Data Collection Job* on page 1289
- *Deleting a Data Collection Job* on page 1290
- *Resuming and Suspending a Data Collection Job* on page 1290
- *Adding a New Schedule to a Job* on page 1291
- *Viewing or Deleting a Schedule* on page 1292
- *Resuming and Suspending the Scheduler* on page 1293
- *Viewing the Job Execution History* on page 1294

Resuming and Suspending the Scheduler

Use the scheduler settings to resume or suspend all scheduled jobs.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

1. From the main menu bar, select **Application > Administration**.
2. In the Sybase Control Center Properties dialog, select **Scheduler**.
3. Do one of the following:
 - To resume the scheduler, click **Resume**.
 - To suspend the scheduler, click **Suspend**.
4. Click **OK**.

See also

- *Executing and Stopping a Data Collection Job* on page 1289
- *Deleting a Data Collection Job* on page 1290
- *Resuming and Suspending a Data Collection Job* on page 1290

- *Adding a New Schedule to a Job* on page 1291
- *Viewing or Deleting a Schedule* on page 1292
- *Modifying the Data Collection Interval for a Job* on page 1293
- *Viewing the Job Execution History* on page 1294

Viewing the Job Execution History

Use the Properties view to display a data collection job's execution history.

1. In the Perspective Resources view, select the resource associated with the job and select **Resource > Properties**.
2. Select **Collection Jobs**.
3. Select a job.
4. Click the **History** tab.

See also

- *Executing and Stopping a Data Collection Job* on page 1289
- *Deleting a Data Collection Job* on page 1290
- *Resuming and Suspending a Data Collection Job* on page 1290
- *Adding a New Schedule to a Job* on page 1291
- *Viewing or Deleting a Schedule* on page 1292
- *Modifying the Data Collection Interval for a Job* on page 1293
- *Resuming and Suspending the Scheduler* on page 1293

Alerts

You can configure Sybase Control Center to notify you when a resource requires attention.

You do this by setting up a predefined alert that is triggered when a performance counter enters a particular state or passes a threshold value that you set. When the alert goes off, it generates an alert notification.

An alert notification takes the form of a visual indicator in the Alert Monitor and, optionally, an e-mail message. The Alert Monitor displays information about the alert, including the resource name, alert severity, value, and date. You can resolve the alert or allow it to escalate.

Configure, monitor, and control alerts for managed resources by:

- Enabling and disabling alert subscriptions for resources
- Configuring shell scripts to run when alerts fire
- Setting alert state or threshold triggers
- Responding to an alert by resolving it, adding notes if desired
- Modifying or deleting alerts

- Viewing alert history

See also

- *Alert-Triggered Scripts* on page 303
- *Creating an Alert* on page 295
- *Assigning a Role to a Login or a Group* on page 119
- *Configuring the E-mail Server* on page 116

Types, Severities, and States

Learn about the properties that define and control alerts.

An alert's type determines what causes it to fire.

Table 46. Alert types

Type	Description
State	A state alert fires when the metric on which it is based changes to a particular state. The possible states are running, pending, stopped, warning, error, and unknown.
Threshold	A threshold alert fires when the metric on which it is based passes a specified level.

Alert severities control when an alert is issued. You can configure the states or threshold values for each alert.

Table 47. Alert severities

Severity	Description
Normal	No alert is issued.
Warning	A problem has given cause for concern. An alert is issued; you can choose whether to subscribe to alerts that fire at the Warning level.
Critical	A serious problem exists. An alert is issued; you can choose whether to subscribe to alerts that fire at the Critical level.

State-based alerts use these states:

- Running
- Pending
- Unknown
- Warning
- Stopped
- Error

The definitions of these states vary by component and sometimes by alert. See the component-specific topics for details.

See also

- *Viewing Alerts* on page 1296
- *Modifying an Alert* on page 1297
- *Testing an Alert-Triggered Script* on page 1297
- *Deleting an Alert* on page 1298
- *Alert Subscriptions* on page 1299
- *Alert Notifications* on page 1301
- *Creating an Alert* on page 295

Viewing Alerts

Display alert notifications and alerts that have been configured for a given resource.

- To display generated alerts (notifications):
 - a) Select **View > Open > Alert Monitor** from the application menu bar.
For a given alert, the Alert Monitor displays only the most recent unresolved notifications at each severity level. That is, if an alert fires five times at the warning level, only the notification of the fifth firing is listed—even if the previous four alerts remain unresolved.
 - b) To display information about a generated alert, select the alert in the Alert Monitor and click **Properties**.
- To display configured alerts:
 - a) In the Perspective Resources view, select a resource and select **Resource > Properties**.
 - b) Click **Alerts** to view configured alerts for the selected resource.
(This is a different route to the information displayed in the second step, above.)

See also

- *Types, Severities, and States* on page 1295
- *Modifying an Alert* on page 1297
- *Testing an Alert-Triggered Script* on page 1297
- *Deleting an Alert* on page 1298
- *Alert Subscriptions* on page 1299
- *Alert Notifications* on page 1301
- *Creating an Alert* on page 295

Modifying an Alert

Use the Properties view of your managed resource to modify an alert.

1. In the Perspective Resources view, select a resource and select **Resource > Properties**.
2. Select **Alerts**.
3. Select the alert to modify.
4. On the Thresholds tab, modify the threshold values. Click **OK** to save your changes.
5. On the Script tab, click **Modify** to change the alert severity at which script execution is triggered, the path to the script, the execution parameters, or the test values. Click **Finish** to save your changes.
6. On the Subscriptions tab, select a subscription and click **Modify** to change its e-mail address or escalation address. Click **Finish** to save your changes.
7. On the Storm Suppression tab, pull down the menu to change the units and enter a value for the storm suppression period.
8. Click **OK** (to apply the changes and close the properties dialog) or **Apply** (to apply the changes and leave the dialog open).

See also

- *Types, Severities, and States* on page 1295
- *Viewing Alerts* on page 1296
- *Testing an Alert-Triggered Script* on page 1297
- *Deleting an Alert* on page 1298
- *Alert Subscriptions* on page 1299
- *Alert Notifications* on page 1301
- *Creating an Alert* on page 295

Testing an Alert-Triggered Script

Execute a script to make sure it works properly.

Prerequisites

Configure an alert with a script.

Task

1. In the Perspective Resources view, select a resource and select **Resource > Properties**.
2. Select **Alerts**.
3. Select the alert to test.
4. On the Script tab, click **Modify**.

5. If the script requires parameter values, click **Select Parameters** to enter them in the **Execution Parameters** box.

You can include a number of predefined substitution parameters, which are replaced by values from the alert. The parameter values are passed on the command line to the script. For the test execution, use values that test all the parameters used by the script. See the substitution parameters topic (linked below) for more information.

Note: When you test a script, Sybase Control Center supplies test values for the **%Severity %** and **%Source_Application%** parameters (“Testing” and “TestScriptExecution,” respectively). Any test values you supply for these parameters are discarded. This prevents the test results from being confused with real script results after testing and in the SCC repository.

6. Click **Test** to perform a test execution of your script.

If your script takes parameters, the test may fail if parameter values are missing or incorrect.

See also

- *Types, Severities, and States* on page 1295
- *Viewing Alerts* on page 1296
- *Modifying an Alert* on page 1297
- *Deleting an Alert* on page 1298
- *Alert Subscriptions* on page 1299
- *Alert Notifications* on page 1301
- *Alert-Triggered Scripts* on page 303
- *Substitution Parameters for Scripts* on page 305
- *Creating an Alert* on page 295

Deleting an Alert

Use the Properties view of your resource to delete an alert.

1. In the Perspective Resources view, select a resource and select **Resource > Properties**.
2. Select **Alerts**.
3. Select an alert and click **Drop**.
4. Click **Yes** to confirm the deletion.

See also

- *Types, Severities, and States* on page 1295
- *Viewing Alerts* on page 1296
- *Modifying an Alert* on page 1297
- *Testing an Alert-Triggered Script* on page 1297
- *Alert Subscriptions* on page 1299

- *Alert Notifications* on page 1301
- *Creating an Alert* on page 295

Alert Subscriptions

When an alert subscription is configured, the alert notifies the specified user or group of users by e-mail message when the alert fires.

You can configure an alert subscription to send e-mail notifications when the alert reaches a severity of warning, a severity of critical, or both.

You can also configure an alert subscription to escalate after a period of time that you specify. If the alert is not resolved within the escalation period, Sybase Control Center e-mails an escalation message to the user or group whose address you provide for escalations, as well as to the primary subscriber. The escalation message is identical to the primary notification message. Sybase recommends that if you configure alert subscriptions to escalate, you do so only for the most urgent alerts, those with a severity of critical.

See also

- *Types, Severities, and States* on page 1295
- *Viewing Alerts* on page 1296
- *Modifying an Alert* on page 1297
- *Testing an Alert-Triggered Script* on page 1297
- *Deleting an Alert* on page 1298
- *Alert Notifications* on page 1301
- *Creating an Alert* on page 295

Adding or Modifying an Alert Subscription

Use the Properties view to subscribe to an alert or edit an alert subscription.

Prerequisites

Specify the e-mail server to which Sybase Control Center will send e-mail alert notifications.

Task

Each alert can support one subscription. To change addresses, modify the alert's existing subscription.

Note: E-mail notifications are sent from an address of the form SybaseControlCenter@yourdomain—for example, SybaseControlCenter@Bigcompany.com. Make sure your mail system does not block or filter that address.

1. In the Perspective Resources view, select a resource and select **Resource > Properties**.

2. Select **Alerts**.
3. Select an alert instance.
4. On the **Subscriptions** tab:
 - Click **Add** to create a subscription, or
 - Select a subscription and click **Modify** to edit an existing subscription
5. Follow the instructions in the Add Alert Subscription wizard.

For both critical and warning alerts:

Table 48. Alert subscription details

Option	Description
E-mail message	To send an e-mail notification when this alert fires, click the E-mail message box and enter the e-mail address of one user or list.
Escalation e-mail	To escalate this alert (by sending an e-mail notification to another address when this alert has not been responded to after a specified period of time), click the Escalation e-mail box and enter the e-mail address of one user or list.
Time period	Enter the amount of time to wait, following the initial alert notification, before Sybase Control Center sends an e-mail notification to the escalation address.

6. Click **Finish**.

See also

- *Unsubscribing from an Alert* on page 1300
- *Enabling and Disabling Alert Subscription* on page 1301

Unsubscribing from an Alert

Use the Properties view to unsubscribe from an alert.

1. In the Perspective Resources view, select a resource and select **Resource > Properties**.
2. Select **Alerts**.
3. Select an alert instance.
4. In the Subscriptions tab, select the alert subscription and click **Drop**.
When you drop a regular subscription, any escalation subscription is also dropped.
However, dropping an escalation does not affect the regular subscription.
5. Click **Yes** to confirm the deletion.

See also

- *Adding or Modifying an Alert Subscription* on page 1299
- *Enabling and Disabling Alert Subscription* on page 1301

Enabling and Disabling Alert Subscription

Use the Properties view to enable and disable alert subscription.

1. In the Perspective Resources view, select a resource and select **Resource > Properties**.
2. Select **Alerts**.
3. Select an alert instance.
4. In the **Subscriptions** tab, select an alert subscription and:
 - To enable subscription, click **Enable**.
 - To disable subscription, click **Disable**, then click **Yes** to confirm.

See also

- *Adding or Modifying an Alert Subscription* on page 1299
- *Unsubscribing from an Alert* on page 1300

Alert Notifications

An alert notification indicates that an alert has been generated.

Alert notifications are produced when alerts fire. An alert fires if the performance indicator on which it is based passes the threshold or state specified for the severity level of warning. If the performance indicator passes the threshold or state specified for the severity level of critical, the alert fires again and another notification is generated.

Detailed alert notifications appear in the Alert Monitor view. In addition, alerts appear as yellow ! symbols in the heat chart. You can set an alert to also send an e-mail message when it fires.

See also

- *Types, Severities, and States* on page 1295
- *Viewing Alerts* on page 1296
- *Modifying an Alert* on page 1297
- *Testing an Alert-Triggered Script* on page 1297
- *Deleting an Alert* on page 1298
- *Alert Subscriptions* on page 1299
- *Creating an Alert* on page 295

Displaying Alert History and Resolutions

Use the Properties view to see historical information about resolved and unresolved alerts.

The History tab on the Alerts page of the Resource Properties view displays information about every time this alert has fired. Each row of the table represents a single notification generated by the selected alert.

Manage Sybase Control Center

The Resolutions tab displays information about alerts that have been resolved (closed) by a Sybase Control Center administrator.

The History and Resolutions tabs display the 100 most recent alerts or alerts for the last 24 hours, whichever is reached first.

1. In the Perspective Resources view, select a resource and select **Resource > Properties**.
2. Select **Alerts**.
3. Select the alert instance.
4. Click the **History** tab.
5. (Optional) Click the **Resolutions** tab.

See also

- *Resolving Alerts* on page 1302

Resolving Alerts

After you address the cause of an alert, resolve it to remove it from the list of active alerts in the Alert Monitor.

Prerequisites

You must be logged in as a user with Sybase Control Center administrative privileges (sccAdminRole) to resolve alerts.

Task

1. In the Perspective Resources view, select a resource and select **Resource > Properties**.
2. In the left pane, select **Alerts**.
3. Select an alert instance in the top table.
4. Click **Resolve**.
5. Enter an explanation of how you resolved the alert.
6. Click **Submit**.

The state of the alert (shown in the State column) changes to Normal. Notifications on this alert disappear from the Alert Monitor.

Note: See the Resolutions tab for details on resolved alerts.

See also

- *Displaying Alert History and Resolutions* on page 1301

Resources

In Sybase Control Center, a resource is a unique Sybase product component or subcomponent. A server is the most common managed resource.

Sybase products comprise many components, including servers, agents, databases, devices, and processes. A managed resource is a product component or subcomponent that Sybase Control Center lets you monitor and administer. Two important tools for resource management are the Resource Explorer and the Perspective Resources view.

- The Resource Explorer lists resources that are registered with Sybase Control Center. The list may include resources that you have not yet added to a perspective. Registration enables Sybase Control Center to connect to the resource, log in, retrieve monitoring data, and issue commands. Resources are registered at the server or agent level, and registering a server or agent also makes Sybase Control Center aware of any subcomponents. You can register resources individually or register several at once by importing them in a batch.
- The Perspective Resources view lists registered resources that you have added to the current perspective. You must add a resource to a perspective to manage and monitor its availability and performance.

See also

- *Registering an SAP Sybase IQ Server* on page 130
- *Importing Resources for Batch Registration* on page 277

Unregistering a Resource

Remove one or more servers or other resources from Sybase Control Center.

1. From the Sybase Control Center toolbar, click the **Launch Resource Explorer** icon.
2. In the Resource Explorer, select the resources you want to unregister. Use **Shift+click** or **Control+click** to select multiple resources.
3. Select **Resources > Unregister**.
4. Click **Yes** to confirm the removal.

See also

- *Adding a Resource to a Perspective* on page 1304
- *Removing a Resource from a Perspective* on page 1304
- *Modifying a Resource's Name and Connection Properties* on page 1305
- *Searching for Resources in the Resource Explorer* on page 1306
- *Registering an SAP Sybase IQ Server* on page 130
- *Importing Resources for Batch Registration* on page 277

Adding a Resource to a Perspective

Add one or more resources to the current perspective.

Prerequisites

Register the resources.

Task

Add servers or other resources to a perspective so you can monitor and manage them along with other resources in the same perspective.

1. From the Sybase Control Center toolbar, click the **Launch Resource Explorer** icon.
2. Select the resources to add to your perspective. Use **Shift-click** or **Control-click** to select multiple resources.
3. Perform one of these actions:
 - Select **Resources > Add Resources to Perspective**.
 - Drag and drop resources from the Resource Explorer onto the Perspective Resources view. You can select and drag multiple resources.

See also

- *Unregistering a Resource* on page 1303
- *Removing a Resource from a Perspective* on page 1304
- *Modifying a Resource's Name and Connection Properties* on page 1305
- *Searching for Resources in the Resource Explorer* on page 1306
- *Registering an SAP Sybase IQ Server* on page 130
- *Importing Resources for Batch Registration* on page 277

Removing a Resource from a Perspective

Remove one or more resources from the current perspective.

Removing a resource from a perspective does not unregister the resource; it remains in any other perspectives to which it has been added, and remains accessible in the Resource Explorer.

1. Before removing a resource, make sure it is not in use by an open view.
 - Close any views that display the resource.
 - If you prefer not to close the Administration Console, unselect the resource:
 - a) In the left pane of the Administration Console, click **Resource Selection**.
 - b) Locate the resource in the list and click the box to unselect it.

2. If the Perspective Resources view is not open, click the **Show/Hide Perspective Resources View** icon in the perspective toolbar.
3. In the Perspective Resources view, select the resources to remove. Use **Shift-click** or **Control-click** to select multiple resources.
4. Select **Resource > Remove**.
5. Click **Yes** to confirm the removal.

See also

- *Unregistering a Resource* on page 1303
- *Adding a Resource to a Perspective* on page 1304
- *Modifying a Resource's Name and Connection Properties* on page 1305
- *Searching for Resources in the Resource Explorer* on page 1306
- *Adding a Resource to a Perspective* on page 281

Modifying a Resource's Name and Connection Properties

Change the properties of a resource registered with Sybase Control Center.

1. In the Perspective Resources view, select a resource and select **Resource > Properties**.
2. (Optional) On the General Properties page, modify the name or description of the resource.

Enter the actual name of the managed server, using uppercase and lowercase letters. If the name registered in Sybase Control Center does not exactly match the server name, some monitoring functions, including the topology view, do not work.
3. (Optional) On the Connection Information page, modify:
 - the host name
 - the port number
 - other options for the managed resource
4. Click **OK** (to apply the changes and close the properties dialog) or **Apply** (to apply the changes and leave the dialog open).

See also

- *Unregistering a Resource* on page 1303
- *Adding a Resource to a Perspective* on page 1304
- *Removing a Resource from a Perspective* on page 1304
- *Searching for Resources in the Resource Explorer* on page 1306

Searching for Resources in the Resource Explorer

Search for all your managed resources or narrow your search for a particular resource.

1. Click the **Launch Resource Explorer** icon.
2. If the Filter pane is not visible in the Resource Explorer window, select **View > Filter** from the view's menu bar.
3. Enter your search term in the **Filter string** field.
The search term can be any string that appears in the tabular portion of the Resource Explorer, such as the name, or part of the name, of a server or a resource type (ASE Server, for example).
4. (Optional) Select a filtering setting:
 - **Match case** – search for resources whose displayed data includes the search term, including uppercase and lowercase letters; or
 - **Exact match** – search for resources whose displayed data includes an item identical to the search term.
5. (Optional) Select a column from the **Filter on** list to restrict your search to that column.

See also

- *Unregistering a Resource* on page 1303
- *Adding a Resource to a Perspective* on page 1304
- *Removing a Resource from a Perspective* on page 1304
- *Modifying a Resource's Name and Connection Properties* on page 1305

Perspectives

A perspective is a named container for a set of one or more managed resources. You can customize perspectives to provide the information you need about your environment.

As the main workspaces in the Sybase Control Center window, perspectives let you organize managed resources. You might assign resources to perspectives based on where the resources are located (continents, states, or time zones, for example), what they are used for, which group owns them, or which administrator manages them. Perspectives appear as tabs in the main window.

Every perspective includes a Perspective Resources view, which lists the resources in that perspective and provides high-level status and descriptive information. Use the View menu to switch from detail view to icon view and back.

You can open additional views —the heat chart, statistics chart, or alert monitor, for example — as needed to manage the perspective's resources. The views in a perspective display information only about resources in that perspective.

One resource can appear in many perspectives.

Creating a Perspective

Create a perspective in which you can add and manage resources.

1. From the application menu bar, select **Perspective > Create**.
2. Enter a name for your perspective. The name can contain up to 255 characters.
3. Click **OK**.

See also

- *Removing a Perspective* on page 1307
- *Renaming a Perspective* on page 1307

Removing a Perspective

Delete a perspective window.

1. Select the perspective tab you want to delete.
2. In the main menu bar, select **Perspective > Delete**.
The selected perspective disappears. If there are other perspectives, Sybase Control Center displays one.

See also

- *Creating a Perspective* on page 1307
- *Renaming a Perspective* on page 1307

Renaming a Perspective

Change the name of your perspective.

1. Select the perspective tab you want to rename.
2. From the main menu bar, select **Perspective > Rename..**
3. Enter the new name for your perspective.
4. Click **OK**.

See also

- *Creating a Perspective* on page 1307
- *Removing a Perspective* on page 1307

Views

Use views to manage one or more resources within a perspective.

In Sybase Control Center, views are the windows you use to monitor and manage a perspective's resources. You can re-arrange, tile, cascade, minimize, maximize, and generally control the display of the views in your perspective.

Each perspective includes these views:

- Perspective Resources
- Administration Console
- Heat chart
- Alert monitor
- Component log viewer
- Views that exist for each managed resource. These vary by resource type, but typically include the statistics chart, the properties view, and a monitoring view.

Note: Sybase Control Center views are not related to database views; they serve a completely different purpose.

Managing a View

Open, close, minimize, maximize, or restore a view in the current perspective.

You can:

Task	Action
Open a view	Do one of the following: <ul style="list-style-type: none"> • In the Perspective Resources view, select a resource, click the drop-down arrow to the right of the resource name, and select the view to open. • In the application menu bar, select View > Open and choose a view.
Close a view	Select the view to close. In the application menu bar, select View > Close . You can also click the X in the view's upper right corner.
Maximize a view	Click the box in the view's upper right corner. The view enlarges to fill the entire perspective window. Click the box again to return the view to its former size.
Minimize a view	Click the _ in the view's upper right corner. The view shrinks to a small tab at the bottom of the perspective window.

Task	Action
Minimize all views	In the application menu bar, select View > Minimize All Views .
Restore a view	Click the box on the minimized tab to maximize the view. Click the box again to return the view to its former (smaller) size so you can see other views at the same time.
Bring a view to the front	In the application menu bar, select View > Select and choose the view you want from the submenu.







See also

- *Arranging View Layout in a Perspective* on page 1309

Arranging View Layout in a Perspective

Use the view layout options to manage your perspective space.

Click one of these icons in the Sybase Control Center toolbar:

Icon	Action
	Close All Open Views
	Minimize All Open Views
	Restore All Minimized Views
	Cascade All Open Views
	Tile All Open Views Vertically
	Tile All Open Views Horizontally

In a cascade, views overlap; in tiling arrangements, they do not.

Alternatively, you can arrange view layouts from the Sybase Control Center menu bar. From the menu bar, select **Perspective > Arrange** and select your view layout.

See also

- *Managing a View* on page 1308

Instances

Deploy, remove, refresh, or convert Sybase Control Center server or agent instances running from an installation on a shared disk.

Enabling and Disabling Shared-Disk Mode

Turn on or turn off shared-disk mode, which allows you to run multiple Sybase Control Center agents and servers from a single installation on a shared disk.

Prerequisites

Install Sybase Control Center on a shared disk. See the *Sybase Control Center Installation Guide*.

Task

Shared-disk mode affects the entire installation; do not enable or disable individual instances.

Disabling shared-disk mode leaves the instances' file systems intact under <SCC-install-directory>/instances, but the instances cannot run. If you reenable, the instances are able to run again.

1. Change to SCC-3_2/bin.
2. Enable or disable shared disk mode.

To enable shared disk mode:

```
sccinstance -enable
```

To disable shared disk mode:

```
sccinstance -disable
```

See also

- *Deploying an Instance from a Shared Disk Installation* on page 1311
- *Refreshing or Converting an Instance* on page 1312
- *Removing an Instance* on page 1313
- *Shared-Disk Mode* on page 1314
- *sccinstance Command* on page 1315

Deploying an Instance from a Shared Disk Installation

(Optional) Create a Sybase Control Center server or agent from an installation on a shared disk.

Prerequisites

- Install Sybase Control Center on a shared disk.
- Enable shared-disk mode.

Task

1. Log in to the host on which you plan to run the SCC server or agent.

Note: You can create an instance on one host and run it on another host, but doing so interferes with the predeployment checks run by **sccinstance**. Such a deployment might generate errors (port conflicts, for example). If you are confident that the errors are caused by problems that will not be present on the host where you plan to run the instance, use the **-force** option to create the instance.

2. Change to `SCC-3_2/bin`.
3. Create the instance as an SCC agent if you plan to run a managed server on this host. Create the instance as an SCC server if you plan to manage other Sybase servers from this host.

To create an SCC agent called Boston-agent and configure it to run as a Windows service:

```
sccinstance -create -agent -instance Boston-agent -service
```

To create an SCC server called Boston and configure it to run as a Windows service:

```
sccinstance -create -server -instance Boston -service
```

On UNIX systems, omit the **-service** option.

4. If other SCC instances will run on this host, change the port assignments for the new instance. Change the instance names and port values in the sample commands to suit your environment, but take care to specify ports that are not in use by another SCC instance or any other application or server.

This command changes the port assignments for an SCC agent called myagent:

```
sccinstance -refresh -instance myagent -portconfig  
rmi=8888,jiniHttp=9093,jiniRmi=9096,tds=9997
```

This command changes the port assignments for an SCC server called myserver:

```
sccinstance -refresh -server -instance myserver -portconfig  
rmi=8889,db=3640,  
http=7072,https=7073,jiniHttp=9094,jiniRmi=9097,msg=2002,tds=9996
```

5. (Optional) List the instances deployed from this installation:

```
sccinstance -list
```

6. (Optional) If you are setting up an instance in UNIX, configure it to run as a service. See *Starting and Stopping Sybase Control Center in UNIX*.

Next

When you manage and maintain instances, keep in mind that the directory structure for instances is different from that of singleton installations. In file paths in SCC help, replace SCC-3_2 or <scc-install-directory> with SCC-3_2/instances/<instance-name>.

For example, the path to the log directory, SCC-3_2/log, becomes this for an instance called kalamazoo:

```
SCC-3_2/instances/kalamazoo/log
```

See also

- *Enabling and Disabling Shared-Disk Mode* on page 1310
- *Refreshing or Converting an Instance* on page 1312
- *Removing an Instance* on page 1313
- *Shared-Disk Mode* on page 1314
- *sccinstance Command* on page 1315

Refreshing or Converting an Instance

Refresh a Sybase Control Center server or agent deployed from an installation on a shared disk, or convert between server and agent.

Prerequisites

Shut down the instance.

Task

When you refresh an instance of an SCC server or agent, SCC recopies files from the main installation on the shared disk (SCC-3_2/) into the instance's subdirectories (SCC-3_2/instances/<instance-name>). In Windows, SCC recopies all the files that make up this instance; in UNIX, it recopies all this instance's services and plug-ins.

Refreshing an instance preserves configuration and logs but overwrites the repository, so historical performance data is lost.

As part of a refresh, you can:

- Convert a server to an agent
- Convert an agent to a server

- Reassign ports on the instance

Converting from an agent to a server adds server-related files to the instance; converting from a server to an agent removes files.

1. Change to `SCC-3_2/bin`.
2. Refresh the instance. Change the instance names and port values in the sample commands to suit your environment, but take care to specify ports that are not in use by another SCC instance or any other application or server.

This command refreshes an SCC server called `boston`. If `boston` is an agent, it becomes a server after the refresh.

```
sccinstance -refresh -server -instance boston
```

This command refreshes an SCC agent called `kalamazoo`. If `kalamazoo` is a server, it becomes an agent after the refresh.

```
sccinstance -refresh -agent -instance kalamazoo
```

This command refreshes an SCC agent called `kalamazoo` and reassigns `kalamazoo`'s RMI and TDS ports. If `kalamazoo` is a server, it becomes an agent after the refresh.

```
sccinstance -refresh -agent -instance kalamazoo -portconfig  
rmi=7070,tds=7071
```

3. (Optional) Display the status of the refreshed instance. Replace the name in the sample command with your instance's name, or omit the **-instance** option to display the status of the instance on this host.

```
sccinstance -instance kalamazoo
```

See also

- *Enabling and Disabling Shared-Disk Mode* on page 1310
- *Deploying an Instance from a Shared Disk Installation* on page 1311
- *Removing an Instance* on page 1313
- *Shared-Disk Mode* on page 1314
- *sccinstance Command* on page 1315

Removing an Instance

Delete a Sybase Control Center server or agent deployed from an installation on a shared disk.

Prerequisites

Shut down the instance.

Task

Removing an SCC instance deletes the instance's files and directories (SCC-3_2/instances/<instance-name> and its contents) from the installation.

You cannot restore a removed instance.

1. Change to SCC-3_2/bin.
2. Remove the instance. Change the instance names in the sample commands to suit your environment.

This command removes an SCC server called porcupine if it is not running; if it is running, you see an error.

```
sccinstance -remove -instance porcupine
```

This command removes the SCC agent on the current host if it is not running. If the agent is running, the command returns an error.

```
sccinstance -remove
```

See also

- *Enabling and Disabling Shared-Disk Mode* on page 1310
- *Deploying an Instance from a Shared Disk Installation* on page 1311
- *Refreshing or Converting an Instance* on page 1312
- *Shared-Disk Mode* on page 1314
- *sccinstance Command* on page 1315

Shared-Disk Mode

Shared-disk mode lets you run multiple Sybase Control Center instances—SCC servers, SCC agents, or a mixture of the two—from a single installation of the product.

The shared-disk capability enables SCC servers or agents on the installation host or on remote hosts to access and execute from the same installation. This feature is especially useful if you plan to use SCC to manage Adaptive Server® clusters, SAP Sybase ESP clusters, or SAP Sybase IQ multiplexes.

After installing SCC on a shared disk, use the **sccinstance** command to enable shared-disk mode and deploy instances. **sccinstance** copies the files needed for the instance into a new directory structure. The path takes the form <SCC-install-directory>/instances/<instance-name> (for example, SCC-3_2/instances/SCCserver-1).

You can specify a name for each instance. If you do not supply a name, the instance name defaults to the host name.

An instance runs on the host on which you start it. When shared-disk mode is enabled, SCC servers and agents run out of the `SCC-3_2/instances` subdirectories, not from the base file system.

In shared-disk mode, changes made to configuration files in the base file system (everything under `SCC-3_2` except the `SCC-3_2/instances` branch) are copied to any instance deployed thereafter. Previously deployed instances are not affected.

Use **sccinstance** to deploy, remove, refresh, or convert an instance; to configure an instance's ports; and to configure a Windows instance to run as a service. Perform other tasks, including configuring a UNIX instance to run as a service, and all other configuration, using the tools and procedures documented for all installations. Use tools provided by the UI wherever possible. When you must edit a file to change the configuration of an instance (for role mapping, for example), edit the copy of the file stored under `<SCC-install-directory>/instances/<instance-name>`.

See also

- *Enabling and Disabling Shared-Disk Mode* on page 1310
- *Deploying an Instance from a Shared Disk Installation* on page 1311
- *Refreshing or Converting an Instance* on page 1312
- *Removing an Instance* on page 1313
- *sccinstance Command* on page 1315

sccinstance Command

Use **sccinstance.bat** (Windows) or **sccinstance** (UNIX) to deploy an instance of Sybase Control Center from a shared-disk installation or to manage existing instances.

You can run multiple instances of Sybase Control Center, including SCC servers, SCC agents, or a mixture of the two, from a single installation on a shared disk.

Syntax

```
sccinstance[.bat]
[-agent]
[-c | -create]
[-d | -debug]
[-disable]
[-enable]
[-f | -force]
[-h | -help]
[-host host-name]
[-i | -instance [instance-name]]
[-l | -list]
[-plugins {plugin-ID,plugin-ID,...}]
[-portconfig {port-name=port-number,port-name=port-number, ...}]
[-refresh]
[-r | -remove]
[-s | -server]
```

```
[-service]  
[-silent]
```

Parameters

- **-agent** – use with **-create** or **-refresh** to create or refresh an SCC agent. In a **-create** or **-refresh** command, **-agent** is the default, so you can omit it.
- **-create** – deploy a new instance. Use alone or with **-agent** to create an agent instance, or with **-server** to create a server instance.
- **-d** | **debug** – display debugging messages with the output of this command.
- **-disable** – turn off shared-disk mode for this installation. Generates an error if any instance is running.
- **-enable** – turn on shared-disk mode for this installation. Shared-disk mode is required if you intend to run more than one server or agent from a single installation of SCC.
- **-f** | **-force** – execute **sccinstance** even if there are potential conflicts, such as port clashes or a running SCC process. Sybase does not recommend using **-force** to remove or refresh a running instance in a Windows environment.
- **-h** | **--help** – display help and usage information for the **sccinstance** command.
- **-host** *host-name* – specify the host for this instance. Use with **-create**; required only when the instance name does not match the name of the host on which this instance will run. (The instance name defaults to the name of the current host unless you use **-instance** to specify another name.)
- **-instance** [*instance-name*] – specify an instance. Use with **-create**, **-remove**, or **-refresh**, or use alone to display the instance's status. You can omit **-instance** when you are addressing the only SCC instance or the only instance of the specified type (server or agent) on the current host.

sccinstance assumes that the host name is the same as the instance name unless you use **-host** to specify a different host name.

- **-l** | **-list** – display a list of all instances deployed from this SCC installation.
- **-plugins** {*plugin-ID,plugin-ID,...*} – specify one or more product module plug-ins for this instance. An alternative to **-agent** and **-server**, **-plugins** is primarily for use by the SCC installation program. Use with **-create** or **-refresh**. Use commas to separate plug-in names.
- **-portconfig** {*port-name=port-number, port-name=port-number, ...*} – assign ports to services for this instance. Use only with **-create** or **-refresh**. For the *port-name* value, use a port name from the table below. If you plan to run more than one SCC instance on a host machine, you must reassign all the ports for every instance after the first.

Port information:

Port Name	Description	Service Names	Property Names	Default Port
db	Database port Present on SCC server	SccSADataserver Messaging Alert Scheduler	com.sybase.asa.server.port messaging.db.port alert.database.port org.quartz.data-Source.ASA.URL	3638
http	Web HTTP port Present on SCC server	EmbeddedWebCon- tainer	http.port	8282
https	Web HTTPS (secure HTTP) port Present on SCC server	EmbeddedWebCon- tainer	https.port	8283
jiniHttp	JINI HTTP server Present on SCC server and SCC agent	Jini	httpPort	9092
jiniR- mid	JINI remote method in- vocation daemon Present on SCC server and SCC agent	Jini	rmidPort	9095
msg	Messaging port Present on SCC server	Messaging	messaging.port	2000
rmi	RMI port Present on SCC server and SCC agent	RMI	port	9999
tds	Tabular Data Stream™ port (used to communi- cate with other Sybase products) Present on SCC server and SCC agent	Tds	tdsPort	9998

- **-refresh** – recopy all the files that make up this instance (Windows) or all this instance's services and plug-ins (UNIX). Refreshing preserves any service or plug-in configuration in the deployed instance.

You can also use **-refresh** to convert a server to an agent or an agent to a server (see the examples). Files are removed or added to change the function of the instance. Use alone or

with **-agent** to refresh an agent instance, or with **-server** to refresh a server instance. Generates an error if the instance is running.

- **-r | -remove** – delete an instance. Use alone or with **-instance**. Generates an error if the instance is running. You cannot restore a removed instance.
- **-s | -server** – use with **-create** or **-refresh** to create or refresh an SCC server, including any product modules available.
- **-service** – use with **-create** or **-remove** to create or remove a Windows service for this instance. You must be logged in to Windows as an administrator to use this option.
- **-silent** – suppress the output of **sccinstance**.

Examples

- **Deploy an SCC server instance** – enables shared-disk mode, deploys a server called Boston with a Windows service on the current host, and starts the Windows service:

```
sccinstance -enable
sccinstance -create -server -instance Boston -service
net start "Sybase Control Center 3.2.3 (Boston)"
```

Note: To create the service, you must log in to Windows as an administrator.

- **Deploy an SCC agent instance** – deploys an SCC agent on this host and configures a Windows service for it. The **-agent** option, because it is the default, is not required—the command does exactly the same thing without it.

```
sccinstance -create -agent -service
```

or

```
sccinstance -create -service
```

- **Deploy a server instance and reassign ports** – deploys the server on this host and configures nondefault RMI, HTTP, and HTTPS ports.

```
sccinstance -create -server -portconfig
rmi=8888,http=7070,https=7071
```

- **Deploy two instances on the same host** – creates two agent instances on the host fireball. The first command does not need the **-host** option because the instance name is the same as the host name.

```
sccinstance -create -agent -instance fireball -portconfig rmi=9991
sccinstance -create -agent -instance fireball2 -host fireball
-portconfig rmi=9992
```

Note: In a production environment, Sybase recommends that you deploy no more than one SCC instance of each type (one server and one agent) on the same host.

- **Refresh a server instance or convert an agent to a server** – refreshes the server on this host. If the instance on this host is an SCC agent, refreshing it as an SCC server converts it into a server.

```
sccinstance -refresh -server
```

- **Refresh an agent instance or convert a server to an agent** – refreshes the instance named kalamazoo. If kalamazoo is a server, refreshing it as an SCC agent converts it into an agent.

```
sccinstance -refresh -agent -instance kalamazoo
```

- **Remove a server instance** – removes the instance named porcupine if it is not running:

```
sccinstance -remove -instance porcupine
```

- **Display status** – displays the status of the instance on this host:

```
sccinstance
```

- **List all instances** – displays a list of all SCC server and agent instances deployed from this SCC installation:

```
sccinstance -list
```

- **Scenario: Remove an instance by force** – suppose you have inadvertently deployed two SCC agent instances on the same host:

```
$ sccinstance -list
2 SCC instances deployed:
SCC instance node1 deployed in agent mode for host node1 RMI port
9999
SCC instance node2 deployed in agent mode for host node2 RMI port
9999
```

Both instances use the same RMI port. You must either reassign ports for one instance or remove it. But you get an error if you try remove an instance when another instance is running on the same host:

```
$ sccinstance -instance node2 -remove
[ERROR] Command execution failed.
[ERROR] SCC instance node2 could not be removed because it is
running. Shut
down the SCC before removing the instance.
```

Use the **-force** option to override the error and force the removal of the second agent instance:

```
$ sccinstance -instance node2 -remove -force
Removing SCC instance node2 ...
SCC instance node2 was successfully removed.
```

Permissions

sccinstance permission defaults to all users, except as noted for certain parameters.

See also

- *Enabling and Disabling Shared-Disk Mode* on page 1310
- *Deploying an Instance from a Shared Disk Installation* on page 1311

- *Refreshing or Converting an Instance* on page 1312
- *Removing an Instance* on page 1313
- *Shared-Disk Mode* on page 1314

Repository

The Sybase Control Center embedded repository stores information related to managed resources, as well as user preference data, operational data, and statistics.

You can back up the repository database on demand, schedule automatic backups, restore the repository from backups, and configure repository purging options. Full and incremental backups are available. A full backup copies the entire repository. An incremental backup copies the transaction log, capturing any changes since the last full or incremental backup.

By default, Sybase Control Center saves backups as follows:

- Each full backup is stored in its own subdirectory in `SCC-3_2/backup`.
- Each incremental backup is stored in a file in `SCC-3_2/backup/incremental`.

Sybase recommends that you periodically move backup files to a secondary storage location to prevent the installation directory from becoming too large.

Scheduling Backups of the Repository

Configure full and incremental backups of the repository to occur automatically.

Prerequisites

Determine your backup strategy, including when to perform full backups and incremental backups. For example, you might schedule incremental backups every day and a full backup every Saturday.

You must have administrative privileges (`sccAdminRole`) to perform this task.

Task

A full backup copies the entire repository. An incremental backup copies the transaction log, capturing any changes since the last full or incremental backup.

1. From the main menu, select **Application > Administration**.
2. In the left pane, select **Repository**.
3. Click the **Full Backup** tab.
4. (Optional) To change the directory in which backups will be stored, click **Browse** and navigate to the desired directory.
5. Select **Schedule a Regular Backup**.

6. Specify the day you want scheduled backups to begin. Enter a **Start date** or click the calendar and select a date.
7. (Optional) Use the **Time** and **AM/PM** controls to specify the time at which backups occur.
8. Specify how often backups occur by setting the **Repeat interval** and selecting hours, days, or weeks.
9. (Optional) To purge the repository after each backup, select **Run a repository purge after the backup completes**.
10. If you include purging in the backup schedule, go to the **Size Management** tab and unselect **Automatically purge the repository periodically** to disable automatic purging.
11. Click **Apply** to save the schedule.
12. Click the **Incremental Backup** tab and repeat the steps above to schedule incremental backups to occur between full backups.

Next

Set purging options on the Size Management tab.

See also

- *Modifying the Backup Schedule* on page 1321
- *Forcing an Immediate Backup* on page 1322
- *Restoring the Repository from Backups* on page 1323
- *Configuring Repository Purging* on page 1324

Modifying the Backup Schedule

Suspend or resume repository backups or change the backup schedule.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

1. From the main menu, select **Application > Administration**.
2. In the left pane, select **Repository**.
3. Choose the type of backup to modify:
 - Click the **Full Backup** tab, or
 - Click the **Incremental Backup** tab.
4. (Optional) To suspend or resume the backup schedule, select or unselect **Schedule a Regular Backup**.

When you unselect (uncheck) this option, the scheduling area is grayed out and scheduled backups no longer occur. However, the schedule is preserved and you can reinstate it at any time.

5. To change the backup schedule, edit the **Start date**, **Time**, **Repeat interval**, or units. You can also select or unselect **Run a repository purge after the backup completes**.
6. Click **Apply** to save the schedule.

See also

- *Scheduling Backups of the Repository* on page 1320
- *Forcing an Immediate Backup* on page 1322
- *Restoring the Repository from Backups* on page 1323
- *Configuring Repository Purging* on page 1324

Forcing an Immediate Backup

Perform an unscheduled full or incremental backup of the repository.

Prerequisites

You must have administrative privileges (sccAdminRole) to perform this task.

Task

1. From the main menu, select **Application > Administration**.
2. In the left pane, select **Repository**.
3. Choose the type of backup to run:
 - Click the **Full Backup** tab, or
 - Click the **Incremental Backup** tab.
4. Click **Back up Now**.

Sybase Control Center saves the backup to the directory shown in the Location field.

See also

- *Scheduling Backups of the Repository* on page 1320
- *Modifying the Backup Schedule* on page 1321
- *Restoring the Repository from Backups* on page 1323
- *Configuring Repository Purging* on page 1324

Restoring the Repository from Backups

Load backup files into the repository database to revert undesirable changes or to recover from a catastrophic failure.

If you configured Sybase Control Center to store backups somewhere other than the default location, change the source directory in the copy commands in this procedure.

1. Shut down Sybase Control Center.
2. Copy the most recent full backup from SCC-3_2/backup/
<generated_directory_name> to SCC-3_2/services/Repository. For example:

Windows:

```
copy C:\sybase\SCC-3_2\backup\repository.  
270110161105\scc_repository.db  
C:\sybase\SCC-3_2\services\Repository
```

UNIX:

```
cp /opt/sybase/SCC-3_2/backup/repository.270110161105/  
scc_repository.db  
/opt/sybase/SCC-3_2/services/Repository
```

3. If you have no incremental backups to load,
 - a) Also copy the log file from SCC-3_2/backup/
<generated_directory_name> to SCC-3_2/services/Repository.
For example:

Windows:

```
copy C:\sybase\SCC-3_2\backup\repository.  
270110161105\scc_repository.log  
C:\sybase\SCC-3_2\services\Repository
```

UNIX:

```
cp /opt/sybase/SCC-3_2/backup/repository.270110161105/  
scc_repository.log  
/opt/sybase/SCC-3_2/services/Repository
```

- b) Skip to step 5 on page 1324.
4. (Optional) To load incremental backups, start the repository database using the **-ad** option, which directs it to load transaction logs (incremental backups) from the incremental directory. (The database loads full backups automatically.) For example:

Windows:

```
cd sybase\SCC-3_2\services\Repository  
  
..\..\bin\sa\bin_<platform>\dbsrv11.exe scc_repository -ad  
sybase\SCC-3_2\backup\incremental
```

UNIX:

Manage Sybase Control Center

```
cd /opt/sybase/SCC-3_2/services/Repository

../../bin/sa/bin <platform>/dbsrv11 scc_repository -ad
/opt/sybase/SCC-3_2/backup/incremental
```

The repository database loads the full backup and any subsequent incremental backups present in the `incremental` directory. Incremental backups are loaded in date order. After loading and saving, the database shuts down.

5. Start Sybase Control Center.

If you loaded incremental backups, Sybase Control Center starts normally (that is, no further recovery occurs). If you copied a full backup to the `Repository` directory, the database recovers the repository from the full backup.

Example: Loading incremental backups into the repository database

These commands start SQL Anywhere® on a 32-bit Windows machine:

```
% cd C:\sybase\SCC-3_2\services\Repository
% ../../bin\sa\bin_windows32\dbsrv11.exe scc_repository -ad
C:\sybase\SCC-3_2\backup\incremental
```

These commands start SQL Anywhere on a 64-bit machine running Solaris:

```
$ cd /opt/sybase/SCC-3_2/services/Repository
$ ../../bin/sa/bin_sunsparc64/dbsrv11 scc_repository -ad
/opt/sybase/SCC-3_2/backup/incremental
```

See also

- *Scheduling Backups of the Repository* on page 1320
- *Modifying the Backup Schedule* on page 1321
- *Forcing an Immediate Backup* on page 1322
- *Configuring Repository Purging* on page 1324

Configuring Repository Purging

Change repository purging options.

Prerequisites

You must have administrative privileges (`sccAdminRole`) to perform this task.

Task

As you decide how to purge your repository, consider that:

- Purging keeps the repository from absorbing too much disk space.
- By default, purging is enabled. It occurs once a day and purges data older than one day.
- Statistics and alert history can help you detect trends in server performance and user behavior. The Sybase Control Center statistics chart can graph performance data over a

period of a year or more if the data is available. If you have enough disk space, consider saving data for a longer period of time or disabling the purging of statistics or alert history.

- Changing the purge frequency and other options might affect Sybase Control Center performance.

Note: If you configure purging as part of a scheduled backup of the repository, disable automatic purging on the Size Management tab.

1. From the main menu bar, select **Application > Administration**.
2. Select **Repository**.
3. Click the **Size Management** tab.
4. To turn automatic purging on or off, click **Automatically purge the repository periodically**.
Turn this option off if purging is configured as part of your scheduled full or incremental backups.
5. Click purge options to turn them on or off:
 - **Purge statistics**
 - **Purge alert history**
6. In **Purge data older than**, enter the number of days after which to purge repository data.
7. Click **Apply**, then **OK**.

See also

- *Scheduling Backups of the Repository* on page 1320
- *Modifying the Backup Schedule* on page 1321
- *Forcing an Immediate Backup* on page 1322
- *Restoring the Repository from Backups* on page 1323

Logging

Logging helps Sybase Control Center administrators identify and track errors and other system events by recording messages about the events in log files.

Sybase Control Center maintains these logs:

- The client log – captures messages about activities in the browser-based client components. These messages are generated by the component product modules to display information that is pertinent to the user but not critical enough to warrant a pop-up. Sybase also uses the client log to trace client browser operations.
- Server logs – capture messages about activities during the initialization sequence, such as starting services; auditing messages recording logins and logouts; errors such as missed scheduled events; and other events on the server. Server logs include:

- Component logs, which record only events concerning individual product modules
- The SCC agent log, which is a composite log. In an SCC server, the agent log records events in all product modules and in the Sybase Control Center framework. In an SCC agent, the agent log records events in the agent.
- The repository log – captures information about inserts and updates that have occurred in the Sybase Control Center repository, a SQL Anywhere database. This log is in `SCC-3_2\log\repository.log`.
- The alert services log – captures information about alert service status and events, including execution of alert-triggered scripts (start time, end time, and status and exit codes). This log is in `SCC-3_2\log\alert-server.log`.

Viewing the Sybase Control Center for Sybase IQ Log

View event logs for Sybase Control Center for Sybase IQ.

Sybase Control Center for Sybase IQ uses Log4J for message logging. The Sybase Control Center for Sybase IQ log files are located at:

- Windows – `%SYBASE%\SCC-3_2\plugins\IQMAP\log\iqmap.log`
- UNIX – `$SYBASE/SCC-3_2/plugins/IQMAP/log/iqmap.log`

1. Display the log file using a log viewer or another method of your choice.
2. Look for entries of interest such as login attempts or the failure of a service to start.

See also

- *Modifying the Sybase IQ Log Configuration* on page 1326
- *Using the SAP Sybase IQ Server and SCC Agent Logs* on page 1327
- *Viewing Sybase Control Center Server Logs* on page 1329
- *Viewing the Sybase Control Center Client Log* on page 1329
- *Changing the Logging Level* on page 1330
- *Logging or Message Levels* on page 1331
- *Changing Logging Configuration* on page 1331

Modifying the Sybase IQ Log Configuration

Change the log level or logging configuration settings for Sybase Control Center for Sybase IQ.

1. Navigate to `%SYBASE%\SCC-3_2\plugins\IQMAP`.
2. Open the `IQMapLog4j.properties` file, and modify the settings as needed.
3. Save and close the `IQMapLog4j.properties` file.
4. Restart the SCC server.

Messages related to SCC for Sybase IQ are recorded on the console and the `iqmap.log` file. The `iqmap.log` file is located in `%SYBASE%\SCC-3_2\plugins\IQMAP\log`.

See also

- *Viewing the Sybase Control Center for Sybase IQ Log* on page 1326
- *Using the SAP Sybase IQ Server and SCC Agent Logs* on page 1327
- *Viewing Sybase Control Center Server Logs* on page 1329
- *Viewing the Sybase Control Center Client Log* on page 1329
- *Changing the Logging Level* on page 1330
- *Logging or Message Levels* on page 1331
- *Changing Logging Configuration* on page 1331

Using the SAP Sybase IQ Server and SCC Agent Logs

View, filter, copy, and paste from SAP Sybase IQ server and SCC agent log snapshots in the Administration Console.

Prerequisites

To view the SAP Sybase IQ server and SCC agent logs, you must authenticate the server (in Perspective Resources). To view the SCC agent log, you must also authenticate the SCC agent.

Task

The SAP Sybase IQ server log records startup errors, tracks verification processes, and may help diagnose multiplex synchronization issues. If you log server requests, the log may also help resolve query problems.

The SCC agent log records SCC agent activities and may help diagnose issues. Various logging levels are available to record corresponding information. In order of priority, these levels are ALL < TRACE < DEBUG < INFO < WARN < ERROR < FATAL < OFF. The default logging level, INFO, records all informational, warning, error, and fatal messages.

The SCC agent log provides diagnostic information for the agent, and its DEBUG setting provides extra detail.

You can:

Task	Action
Open a log	<p>Do one of the following:</p> <ul style="list-style-type: none"> Expand the IQ Servers tree and select a server in the right panel. From a server's Resource menu, click View Server Log or View Agent Log. Expand the Multiplex Management tree in the left panel and click Multiplex Servers. Select a multiplex server in the right panel and click View Server Log or View Agent Log. Expand the IQ Servers tree and select a multiplex server in the right panel. From a server's Resource menu, click Properties. From the Multiplex Properties window that opens, select Multiplex Servers from the tree menu. Select a multiplex server in the right panel and click View Server Log or View Agent Log.
Filter logs	In the log window, click the Settings button on the top right corner. Choose a setting and click Apply Settings .
Copy and paste rows or the table	<p>In the log window, do one of the following:</p> <ul style="list-style-type: none"> Click the Copy Rows button on the top right. Click the Copy Table button on the top right.

The SAP Sybase IQ server and SCC agent logs are static snapshots that do not refresh automatically. Close and reopen the log window to view a refreshed snapshot.

See also

- *Viewing the Sybase Control Center for Sybase IQ Log* on page 1326
- *Modifying the Sybase IQ Log Configuration* on page 1326
- *Viewing Sybase Control Center Server Logs* on page 1329
- *Viewing the Sybase Control Center Client Log* on page 1329
- *Changing the Logging Level* on page 1330
- *Logging or Message Levels* on page 1331
- *Changing Logging Configuration* on page 1331

Viewing Sybase Control Center Server Logs

View event logs for the Sybase Control Center server.

Sybase Control Center logs events to several places:

- The console from which Sybase Control Center is launched.
- The Sybase Control Center agent log: <SCC-install-directory>/log/agent.log
- The repository log: <SCC-install-directory>/log/repository.log
- The component log for each installed Sybase Control Center product module. The path to the component log takes this form: <SCC-install-directory>/plugins/<component>/log/<component>.log

1. Display one of the log files using a log viewer or a method of your choice.
2. Look for entries of interest such as login attempts or the failure of a service to start.

On the console and in the Sybase Control Center agent log file, some components prepend the component name to log entries.

See also

- *Viewing the Sybase Control Center for Sybase IQ Log* on page 1326
- *Modifying the Sybase IQ Log Configuration* on page 1326
- *Using the SAP Sybase IQ Server and SCC Agent Logs* on page 1327
- *Viewing the Sybase Control Center Client Log* on page 1329
- *Changing the Logging Level* on page 1330
- *Logging or Message Levels* on page 1331
- *Changing Logging Configuration* on page 1331

Viewing the Sybase Control Center Client Log

Display the event log for the current session of your Sybase Control Center browser client.

In the perspective tab window (the main window), do either of the following to display the client log:

- Enter **Ctrl+Alt+L**.
- Select **View > Open > Log Window**.

Note: The client log reader displays the 100 most recent log messages for the current login session.

See also

- *Viewing the Sybase Control Center for Sybase IQ Log* on page 1326
- *Modifying the Sybase IQ Log Configuration* on page 1326

- *Using the SAP Sybase IQ Server and SCC Agent Logs* on page 1327
- *Viewing Sybase Control Center Server Logs* on page 1329
- *Changing the Logging Level* on page 1330
- *Logging or Message Levels* on page 1331
- *Changing Logging Configuration* on page 1331

Changing the Logging Level

Adjust the logging level that determines which events Sybase Control Center records in the server logs. This task requires you to restart Sybase Control Center.

If you are having a problem with Sybase Control Center, you might be able to discover the cause of the problem by changing the server logging level so that more events are recorded.

1. Shut down Sybase Control Center.
2. Restart Sybase Control Center using the -m option to change the logging level. In <SCC-installation-dir>/bin, enter:

```
scc -m <logging-level>
```

The logging levels are OFF (logs nothing), FATAL (logs only the most severe events), ERROR, WARN, INFO, DEBUG, and ALL (logs everything).

3. Examine the server log for clues about what might be causing the problem.
4. When you have resolved the problem, set the logging level back to WARN, the default. Your log may become unmanageably large if you leave it at the DEBUG or ALL level.

Example

These commands, which must be executed in the installation directory, start Sybase Control Center with the logging level set to debug:

```
Windows: bin\scc -m DEBUG  
UNIX: bin/scc -m DEBUG
```

See also

- *Viewing the Sybase Control Center for Sybase IQ Log* on page 1326
- *Modifying the Sybase IQ Log Configuration* on page 1326
- *Using the SAP Sybase IQ Server and SCC Agent Logs* on page 1327
- *Viewing Sybase Control Center Server Logs* on page 1329
- *Viewing the Sybase Control Center Client Log* on page 1329
- *Logging or Message Levels* on page 1331
- *Changing Logging Configuration* on page 1331
- *Starting and Stopping Sybase Control Center in Windows* on page 81
- *Starting and Stopping Sybase Control Center in UNIX* on page 84

Logging or Message Levels

Describes values you can use to control the types of events that are logged by Sybase Control Center.

These are the logging levels, from highest to lowest. The higher the level, the more serious an event must be to be logged. Each level includes all the levels above it—for example, if you set the logging level to **WARN**, you log events for the **WARN**, **ERROR**, and **FATAL** levels.

OFF	Nothing is logged. This is the highest level.
FATAL	Logs only very severe error events that lead the server to abort. This is the highest level at which events are logged.
ERROR	Logs error events that might allow the server to continue running.
WARN	Logs potentially harmful situations. WARN is the default logging level during normal operation (that is, after system initialization).
INFO	Logs informational messages that track the progress of the server in a coarse-grained fashion. INFO is the default logging level during the system initialization process.
DEBUG	Logs a larger set of events that provides a finer-grained picture of how the server is operating. This level is recommended for troubleshooting.
ALL	Logs all loggable events. This is the lowest level.

See also

- *Viewing the Sybase Control Center for Sybase IQ Log* on page 1326
- *Modifying the Sybase IQ Log Configuration* on page 1326
- *Using the SAP Sybase IQ Server and SCC Agent Logs* on page 1327
- *Viewing Sybase Control Center Server Logs* on page 1329
- *Viewing the Sybase Control Center Client Log* on page 1329
- *Changing the Logging Level* on page 1330
- *Changing Logging Configuration* on page 1331
- *scc Command* on page 91

Changing Logging Configuration

Edit the logging configuration file, `log4j.properties`, to modify Sybase Control Center logging.

You can change the names, locations, or maximum size of the log files as well as the number of log files backed up.

Options for the **scc** command let you change the overall Sybase Control Center log message level when you start SCC, but if you choose the **DEBUG** level, the large volume of log

messages generated may be inconvenient. Editing the log properties file gives you finer control; you can set logging levels for each Sybase Control Center component separately. Sybase recommends making such changes only if you are familiar with log4j and you are working with Sybase technical support; DEBUG-level log messages are not likely to be meaningful to you. (If you have not used log4j before, a good place to start is <http://logging.apache.org/log4j/1.2/manual.html>.)

1. Shut down Sybase Control Center.
2. Make a backup copy of the `log4j.properties` file located in `<SCC-installation-directory>/conf`.
3. Open the `log4j.properties` file for editing.
4. Change values in the file to suit your needs. For example:

To	Modify
Change the name or location of a log file	<ul style="list-style-type: none">• Agent log – <code>log4j.appender.agent.File</code>• Repository log – <code>log4j.appender.repository.File</code>• Collection statistics log – <code>log4j.appender.collection-stats.File</code>• Alert server log – <code>log4j.appender.alert.File</code>• Gateway log – <code>log4j.appender.gateway.File</code>
Change the maximum size that a log file can reach before Sybase Control Center creates a new file	<ul style="list-style-type: none">• Agent log – <code>log4j.appender.agent.MaxFileSize</code>• Repository log – <code>log4j.appender.repository.MaxFileSize</code>• Collection statistics log – <code>log4j.appender.collection-stats.MaxFileSize</code>• Alert server log – <code>log4j.appender.alert.MaxFileSize</code>• Gateway log – <code>log4j.appender.gateway.MaxFileSize</code>
Change the number of log files Sybase Control Center backs up before deleting the oldest file	<ul style="list-style-type: none">• Agent log – <code>log4j.appender.agent.MaxBackupIndex</code>• Repository log – <code>log4j.appender.repository.MaxBackupIndex</code>• Collection statistics log – <code>log4j.appender.collection-stats.MaxBackupIndex</code>• Alert server log – <code>log4j.appender.alert.MaxBackupIndex</code>• Gateway log – <code>log4j.appender.gateway.MaxBackupIndex</code>

5. Save and exit the file.
6. Start Sybase Control Center to make the logging changes take effect.

See also

- *Viewing the Sybase Control Center for Sybase IQ Log* on page 1326
- *Modifying the Sybase IQ Log Configuration* on page 1326
- *Using the SAP Sybase IQ Server and SCC Agent Logs* on page 1327
- *Viewing Sybase Control Center Server Logs* on page 1329
- *Viewing the Sybase Control Center Client Log* on page 1329

- *Changing the Logging Level* on page 1330
- *Logging or Message Levels* on page 1331
- *Starting and Stopping Sybase Control Center in Windows* on page 81
- *Starting and Stopping Sybase Control Center in UNIX* on page 84

Sybase Control Center Console

The console is a command-line interface for displaying details about the status of the Sybase Control Center server and its subsystems.

When you use the **scc** command to start Sybase Control Center, it displays start-up messages and then displays the console prompt.

Note: The console prompt does not appear if you start Sybase Control Center as a service, if you direct the output of **scc** to a file, or if you start Sybase Control Center in the background.

See also

- *Launching Sybase Control Center* on page 80

Console Commands

Use the Sybase Control Center console to get status information on Sybase Control Center and its ports, plug-ins, and services.

help Command

Display syntax information for one or more Sybase Control Center console commands.

Syntax

```
help [command_name]
```

Parameters

- **command_name** – optional. status, info, or shutdown. If you omit *command_name*, **help** returns information on all the console commands.

Examples

- **Example 1** – returns information on the **status** command:

```
help status
```

Permissions

help permission defaults to all users. No permission is required to use it.

See also

- *info Command* on page 1334
- *shutdown command* on page 1335
- *status Command* on page 1335

info Command

Display information about specified parts of the Sybase Control Center server.

If you enter **info** with no parameters, it returns information for every parameter.

Syntax

```
info [-a | --sys]
[-D | --sysprop [system-property]]
[-e | --env [environment-variable]]
[-h | --help]
[-m | --mem]
[-p | --ports]
[-s | --services]
```

Parameters

- **-a | --sys** – optional. List all the services known to Sybase Control Center, indicate whether each service is enabled, and list other services on which each service depends.
- **-D | --sysprop [system-property]** – optional. Display information about the specified Java system property. Omit the system-property argument to return a list of all Java system properties and their values.
- **-e | --env [environment-variable]** – optional. List all the environment variables in the Sybase Control Center Java VM process environment. Omit the environment-variable argument to return a list of environment variables and their values.
- **-h | --help** – optional. Display information about the **info** command.
- **-m | --mem** – optional. Display information about the server's memory resources.
- **-p | --ports** – optional. List all the ports on which the Sybase Control Center agent and its services listen, indicate whether each port is in use, and show the service running on each port.
- **-s | --services** – optional. List all Sybase Control Center services, indicate whether each service is enabled, and list other services on which each service depends.

Examples

- **Example 1** – displays information about ports on this Sybase Control Center server:

```
info -p
```

Permissions

info permission defaults to all users. No permission is required to use it.

See also

- *help Command* on page 1333
- *shutdown command* on page 1335
- *status Command* on page 1335

shutdown command

Stop the Sybase Control Center server if it is running.

Syntax

```
shutdown
```

Examples

- **Example 1** – shuts down Sybase Control Center:

```
shutdown
```

Permissions

shutdown permission defaults to all users. No permission is required to use it.

See also

- *help Command* on page 1333
- *info Command* on page 1334
- *status Command* on page 1335

status Command

Display the status of the Sybase Control Center agent, plug-in, or service components of Sybase Control Center.

Syntax

```
status [-a | --agent]
[-h | --help]
[-p | --plugin [plugin-name]]
[-s | --service [service-name]]
```

Parameters

- **-a | --agent** – display the status of the Sybase Control Center agent component.

Manage Sybase Control Center

- **-h | --help** – display information about the **info** command.
- **-p | --plugin [plugin-name]** – display the status of the specified Sybase Control Center plug-in (for example, ASEMap, the Adaptive Server® management module). Omit the plugin-name argument to return a list of plug-ins.
- **-s | --service [service-name]** – display the status of the specified Sybase Control Center service (for example, the Alert service or the Messaging service). Omit the service-name argument to return a list of services.

Examples

- **Example 1** – displays status information on the Repository service:

```
status --service Repository
```

Permissions

status permission defaults to all users. No permission is required to use it.

See also

- *help Command* on page 1333
- *info Command* on page 1334
- *shutdown command* on page 1335

Troubleshoot Sybase Control Center for SAP Sybase IQ

Troubleshoot problems that occur in Sybase Control Center for SAP Sybase IQ.

Problems with Basic Sybase Control Center Functionality

Troubleshoot problems that involve basic features like starting and stopping, authentication, alerts, and scheduling.

Cannot Log In

Problem: Cannot log in to Sybase Control Center Web console.

Solution: Make sure that Sybase Control Center has been configured:

- To allow logins through the operating system
- To grant appropriate roles to your login account

Ask the Sybase Control Center administrator to help you check.

See also

- *User Authorization* on page 119
- *Setting Up Security* on page 96

Sybase Control Center Fails to Start

Problem: The Sybase Control Center server does not start.

Solution 1: Port conflict

Solution: SCC might be using one or more ports that are also being used by another server or application on this machine. To check for port conflicts:

1. Execute this command:

```
scc --info ports
```

The command lists all the ports on which Sybase Control Center and its services listen, indicates whether each port is in use, and shows the service running on each port. If SCC is not running, any port shown to be in use represents a conflict.

2. If you discover a conflict, use **scc --port** to change the port used by the Sybase Control Center service.

Solution 2: Insufficient memory

You might see this error why you try to start: Could not create the Java Virtual machine. Increase the maximum memory setting.

See also

- *Configuring Ports* on page 114
- *Configuring Memory Usage* on page 88

Browser Refresh (F5) Causes Logout

Problem: Pressing the **F5** key to refresh your browser logs you out of Sybase Control Center.

Solution: Do not use **F5** when you are logged in to Sybase Control Center. Browser refresh does not refresh data inside Sybase Control Center, but refreshes the loaded application or pages in the browser—in this case, the Adobe Flash on which Sybase Control Center is built. Consequently, pressing **F5** logs you out of any servers you are currently logged in to, including Sybase Control Center.

Alerts Are Not Generated

Problem: Alerts are not being generated in Sybase Control Center.

Solution: Schedule a job to run the data collection that supports your alerts. See the data collections topic for your Sybase Control Center product module for information on which collections must be scheduled.

See also

- *Setting Up Statistics Collection* on page 283

Performance Statistics Do Not Cover Enough Time

Problem: I want to graph performance counters over a long period of time but the statistics chart displays only very recent data.

Solution: Ask your Sybase Control Center administrator to change the repository purging options to keep statistical data available for as long as you need it. By default, statistics are purged frequently to conserve disk space.

See also

- *Configuring Repository Purging* on page 1324
- *Graphing Performance Counters: the Statistics Chart* on page 320

Resetting the Online Help

Problem: Sybase Control Center online help is corrupted or cannot be found (404 error).

Solution: Clear online help files to force SCC to build new ones.

1. Shut down Sybase Control Center.

2. Remove this directory:

```
<SCC-installation-directory>\SCC-3_2\services
\EmbeddedWebContainer\container\Jetty-6.1.22\work
\Jetty_0_0_0_0_8282_help.war__help__.smpe97
```

Tip: In Windows, you might see a deletion error. Regardless of what the errors says, it might be caused by the length of the path. If deletion fails, rename the Jetty_0_0_0_0_8282_help.war__help__.smpe97 folder to something very short, such as J. Then delete the renamed folder.

3. Remove these files:

```
<SCC-installation-directory>\SCC-3_2\services
\EmbeddedWebContainer\container\Jetty-6.1.22\contexts
\_help.xml
<SCC-installation-directory>\SCC-3_2\services
\SybaseControlCenter\help\com.sybase.infocenter.scc.zip
<SCC-installation-directory>\SCC-3_2\services
\SybaseControlCenter\help\help.war
<SCC-installation-directory>\SCC-3_2\services
\SybaseControlCenter\help\help_info.xml
```

4. Start SCC. After the server comes up it rebuilds the help, which takes a few minutes.

5. To display the help, go to <https://<your-SCC-host>:8283/help/index.jsp>.

Note: If you try to display the help too soon after restarting, you get a file not found error. Wait a minute or two and try again.

Data Collections Fail to Complete

Problem: A collection frequently times out or generates errors citing the REJECT_DUPLICATE_RESOURCE_AND_COLLECTION policy, but no problems with the monitored resources are evident.

The errors appear in the log and on the collection history screen.

Solution: Try to determine why the collection is taking so long. For example, are network delays slowing down traffic between Sybase Control Center and the monitored server?

In the case of network delays and other resource-related problems, the interval between collections might be shorter than the time needed to finish the collection. To fix this problem, increase the time between collections.

See also

- *Modifying the Data Collection Interval for a Job* on page 1293

Memory Warnings at Startup

Problem: When Sybase Control Center starts, you see warnings about system memory or heap memory allocation.

Solution: Increase the maximum memory setting (*SCC_MEM_MAX* or *jvmopt=-Xmx*).

See also

- *Configuring Memory Usage* on page 88

SCC Out of Memory Errors

Problem: Sybase Control Center generates *OutOfMemory* errors.

Solution:

- If the *OutOfMemory* error says that Sybase Control Center is out of heap space, increase the maximum memory setting (*SCC_MEM_MAX* or *jvmopt=-Xmx*).
- If the *OutOfMemory* error says that Sybase Control Center is out of permanent generation space, increase the permanent memory setting (*SCC_MEM_PERM* or *jvmopt=-XX:MaxPermSize*).
- Repeated *OutOfMemory* errors may indicate a memory leak. *OutOfMemory* errors generate heap dumps:
 - When Sybase Control Center runs as a service in Windows:
C:/windows/system32
 - When Sybase Control Center runs as a service in UNIX:
<SCC-install-directory>/SCC-3_2/binSend the heap dump files to Sybase technical support for analysis.

See also

- *Configuring Memory Usage* on page 88

Login Fails when Authenticating a Chinese or Japanese SAP Sybase IQ Server

Problem: When authenticating a Chinese or Japanese SAP Sybase IQ server, if the login name or password contain Chinese or Japanese characters, the login fails.

Solution:

1. In the Perspective Resources window, select the Chinese or Japanese server, click the arrow, and select **Properties**.
2. In the Resource Properties window, select **Connection**.

3. Enter the **Character set** used on the SAP Sybase IQ server.
4. Click **OK**.

Feature Disabled on the Administration Console Task Menu

Problem: Some menu options are unavailable when you either select an item in the right pane and click the arrow to the right of the name, or you select **Resource** from the Administration Console menu bar.

This problem occurs if you have not been granted the required system privileges (16.0) or authorities (15.3 and 15.4) to perform an administration task. For some server specific tasks, even if you have been granted the required system privileges or authorities, menu options may still be unavailable if the Sybase Control Center agent is not registered, authenticated, and running.

Solution: Verify that you have been granted the system privileges or authorities required for the authorized task. For server specific tasks, register and authenticate any missing agents and verify that Sybase Control Center is running.

See also

- *Configuring SAP Sybase IQ Roles-Based Users for Monitoring* on page 129
- *Configuring SAP Sybase IQ Authority-Based Users for Monitoring* on page 128

My Database Definition is Invalid

Problem: The Create Databases wizard flags your database definition with a red **x**.

The red **x** indicates that you entered an invalid parameter in your database definition.

Solution: Hover over the red **x** to display an explanation of the invalid parameter. Edit the database definition until the red **x** becomes a green check mark. This table highlights some of the more common causes of an invalid database definition and suggests solutions.

Invalid Database Definition Cause	Solution
Agent not running on port specified.	Correct the agent port.
Database path points to a file that already exists.	Specify a unique database path.
Database path points to a location that is not writeable.	Specify a writeable database path.
Specified IQ port is already in use.	Select a unique port.
Main dbspace path points to a file that already exists.	Specify an unused main dbspace path.

Invalid Database Definition Cause	Solution
Main dbspace path points to a location that is not writeable.	Specify a writeable main dbspace path.
Another database definition with the same name already exists in the wizard list of databases to be created.	Specify a unique database definition.
Temp dbspace path points to a file that already exists.	Specify a unique temp dbspace path.
Temp dbspace path points to a location that is not writeable.	Specify a writeable temp dbspace path.

See *Viewing or Modifying Database Properties* for more detailed information on the requirements of each field.

See also

- *Creating a Database* on page 451
- *Viewing or Modifying Database Properties* on page 457

Sybase Control Center Is Not Controlling My Multiplex Servers

Problem: On an SAP Sybase IQ multiplex installed on a shared disk cluster, you are unable to perform control tasks like starting and stopping the nodes.

This problem occurs when multiple nodes in a multiplex run from the same installation of SAP Sybase IQ. Sybase Control Center monitoring tasks are not affected.

Solution: Use the SAP Sybase IQ installer to install the SCC agent on each machine in the multiplex environment. Sybase Control Center needs a locally installed agent to perform control operations.

Fatal Error #2035 Prevents Me from Logging In

Problem: When trying to connect to Sybase Control Center in Firefox, fatal error #2035 appears before the login screen appears.

Solution:

1. Clear the Firefox cache.
2. Restart Firefox.

3. Enter the SCC URL.
4. Repeat step 3 if required.

Multiplex Node Does Not Appear in Monitor

Problem: One or more multiplex nodes are not visible in the IQ Multiplex Level Monitor view.

The node might not be selected for monitoring. This might be the case when a node has been added or is being monitored by another copy of Sybase Control Center, or when the maximum number of nodes to monitor is set too low.

Solution:

1. In the Perspective Resources view, select the multiplex and click the arrow to the right of its name.
2. Select **Monitor Multiplex**.
3. In the left pane of the monitor view, select **Settings**.
4. In the right pane, make a note of the value displayed for **Maximum number of nodes to show in charts**.
5. Click **Select Nodes**.
6. In the Server column, check the box for the missing node, or click **Select All**.
7. If the number of nodes selected exceeds the value of **Maximum number of nodes to show in charts**:
 - a. Click **Cancel**.
 - b. Increase the value of **Maximum number of nodes to show in charts** and click **Apply**.
8. Return to Select Nodes and check the nodes you want to add.
9. Click **OK**.

Multiplex Connection Disallowed by Login Policy

Problem: If your login cannot access all nodes, authentication returns the security error `Connection disallowed by login policy for this user`.

Solution: Use a login account with access to the SERVER logical server to authenticate a multiplex resource. A connection using the SERVER logical server context requires the ACCESS SERVER LS system privilege.

SQL Anywhere Error -131 Appears When Changing A User's Password

Problem: The error message
`com.sybase.scc.jmx.ManagedObjectGateway.err_invoke_op SQL Anywhere Error -131: Syntax error near 'BY' on line 1` appears when you attempt to change the password of another user.

This error message indicates that the **change_password_dual_control** option is enabled in the login policy for the selected user. This feature is not currently implemented in Sybase Control Center.

Solution: Change the password using interactive SQL.

Note: Once the new dual part password is set, the user must connect to the IQ database outside of Sybase Control Center and change his or her password before he or she can to log in to Sybase Control Center. Failure to do this results in an error when logging in to Sybase Control Center.

Unable to Authenticate After Having Your Password Changed by Another User

Problem: Sybase Control Center does not accept your new password.

This behavior occurs when the dual change password option is enabled for a user, and he or she is attempting to authenticate using the temporary dual part password.

Solution: Connect to the IQ database outside of Sybase Control Center using the dual part password. At the prompt, change your password. Log in to Sybase Control Center and authenticate using your newest password.

Unable to Change Another User's Password

Problem: You are unable to change another user's password, even though you have been granted the CHANGE PASSWORD system privilege.

This behavior may occur if the CHANGE PASSWORD system privilege was granted outside of Sybase Control Center.

When this system privilege is granted using Sybase Control Center, it is granted in such a way to allow you to manage the password of any user. However, when granted outside of Sybase Control Center, the privilege can be limited to allow password management of select users and roles only.

Solution: Check with the IQ database administrator to verify which user passwords you can manage.

Glossary: Sybase Control Center for SAP Sybase IQ

Glossary of Sybase Control Center terms related to SAP Sybase IQ.

alert – a mechanism for notifying administrators when a managed resource experiences a status change, or when a performance metric passes a user-specified threshold.

alert notification – an indication that an alert has fired. Alert notifications appear in the Alert Monitor view. If e-mail notification is enabled, alert notifications are also delivered to the specified e-mail address.

alert storm – the result of issuing many redundant alerts associated with a common or root occurrence. See also alert storm suppression.

alert storm suppression – a Sybase Control Center feature that can be configured to prevent alert storms by suppressing repeat alert notifications for a specified period of time.

alert type – the basis on which an alert fires: state or threshold. State alerts are triggered by the state of their key performance indicator (for example, running or stopped), while threshold alerts are triggered when their KPI's numerical value passes a specified threshold.

authenticate – when SCC authenticates with a managed resource, it logs in to the resource with a user ID and password provided by you. SCC must log in to managed resources in order to gather performance statistics and perform management tasks. You can choose to have SCC use your current SCC login ID, or you can provide different credentials.

availability – indicates whether a resource is accessible and responsive.

catalog store – the portion of each SAP Sybase IQ database that contains its metadata. (Metadata describes the layout of the SAP Sybase IQ tables, columns, and indexes.) The catalog store contains the system dbspace and up to 12 additional catalog dbspaces. The default name for this file is *<dbname>.db*.

chart trend period – the period, in minutes, over which data is displayed in historical charts. Set the chart trend period on the Settings screen of the SAP Sybase IQ Monitoring View. Contrast with screen refresh interval.

collection repeat interval – the period, in seconds, minutes, hours, or days, between successive repetitions of a statistics collection job. The collection repeat interval determines how often new data on historical monitoring screens is available to be refreshed. Set the collection repeat interval in the scheduler. See also screen refresh interval.

collection – a named, predefined set of key performance indicators for which values are collected from monitored servers at the same time. Collections supply the performance and availability data shown on Sybase Control Center screens and charts. Use the scheduler to

view a list of collections and to control which collections run, how often they run, and the length of time for which they run.

connection – a connection from an SAP Sybase IQ server to a database.

database – a collection of tables that are related by primary and foreign keys. The tables hold the information in the database. The tables and keys together define the structure of the database. SAP Sybase IQ databases are specially indexed to take advantage of the query speed of SAP Sybase IQ.

dbspace – a named collection of dbfiles that provides space for data and can be administered as a logical subset of the total storage. The main store, catalog store, and temporary store consist of dbspaces.

event – an activity in the system, such as a user logging in, a service starting or stopping, or a condition changing. Use the alerts feature to detect and notify you about system events.

external environment – a development environment external to SAP Sybase IQ (C/C++ or Java, for example) that you can use to create functions and procedures to run against SAP Sybase IQ databases.

heat chart – a graphical view of resource availability and selected performance and status metrics for all the registered resources in the current perspective.

instance – an SCC agent or server run from a shared disk installation. See also shared-disk mode.

job – a task performed by the scheduler in Sybase Control Center.

key performance indicator (KPI) – a single metric used to evaluate the status or performance of a monitored resource. A KPI value can be a state (such as running, error, or stopped) or a numerical value. KPIs are grouped into collections (and also, for some product modules, into key performance areas, or KPAs). KPI values are collected by scheduled collection jobs and appear on monitoring screens and in the statistics and heat charts. Examples of KPIs are resource state and CPU usage.

key performance area (KPA) – a group of related key performance indicators.

main store – the SAP Sybase IQ main store is the portion of each SAP Sybase IQ database that contains persistent database structures, such as backup metadata and rollback data for committed transactions.

managed resource – see resource.

message row – a row that appears in the right pane of the Administration Console in place of a slow-responding request, a failed request, or a large result set. Rows with slow-responding requests are populated as soon as the data arrives. You can retry failed requests or expand large result sets—select the row and click the drop-down arrow to see options.

multiplex – a powerful feature in SAP Sybase IQ that provides application scalability through a clustered server configuration. An SAP Sybase IQ multiplex is made up of several multiplex

servers, or nodes. Each node is assigned a role: coordinator (one per multiplex), writer, or reader. Readers and writers can serve as secondary nodes, backing up the coordinator node in case of failure. The multiplex feature allows concurrent data loads and queries via independent data processing nodes connected to a shared data source. Each multiplex server has its own catalog store and IQ temporary store; all the servers in the multiplex share a common IQ store. Contrast with simplex.

node – a topology object representing a server or other entity type, displayed in the form of an icon.

perspective – a named tab in Sybase Control Center that displays information related to a collection of managed resources (such as servers) and a set of views associated with those resources. The views in a perspective are chosen by users of the perspective. You can create as many perspectives as you need, and customize them to monitor and manage your resources. Perspectives allow you to group resources in ways that make sense in your environment—for example by location, department, or project.

product module – a plug-in component of Sybase Control Center that manages and monitors a particular Sybase product. SCC product modules are available for Adaptive Server, Data Assurance (a Replication Server option), replication (Replication Server, Replication Agent, and Mirror Replication Agent), Sybase Event Stream Processor, and Sybase IQ.

repository – a database in Sybase Control Center that stores information related to managed resources, along with user preference data, operational data, and performance statistics.

resource – a server, agent, or other entity that can be monitored or administered by Sybase Control Center. Resources SCC can manage include Adaptive Server, Data Assurance Server, Replication Server, Replication Agent, Mirror Replication Agent, Sybase Event Stream Processor, Sybase IQ, and certain subcomponents.

row-level version (RLV) – the unit of versioning is the row. Row-level versioning structures data at the row level of an RLV-enabled table, provided that the RLV dbspace has been created with at least one dbfile. RLV allows row-level updates, inserts, and deletes, by multiple users, in real-time.

SCC-enabled login account – a user account that has been granted privileges in Sybase Control Center by mapping appropriate Sybase Control Center roles. (Roles are typically mapped to a group to which the account belongs rather than to the account itself.) The user account and group can be native to Sybase Control Center or created in the operating system or the LDAP directory service to which Sybase Control Center authentication is delegated. You must use an SCC-enabled account to log in to Sybase Control Center.

SCC agent – a remote command and control agent for Sybase Control Center that runs on a managed server. The SCC agent is installed automatically as part of the Sybase server.

schedule – the definition of a task (such as the collection of a set of statistics) and the time interval at which Sybase Control Center executes the task.

screen refresh interval – the period in seconds between refreshes of screens in the monitor views (IQ Node Level Monitor and IQ Multiplex Level Monitor). Refreshing a screen redraws it with the most recent available data. Set the screen refresh interval on the Settings screen of either monitor view. See also collection repeat interval.

shared-disk mode – a feature that enables multiple instances of Sybase Control Center to execute from a single installation on a shared disk. Instances can be SCC servers, agents, or a mixture of the two.

simplex – an SAP Sybase IQ implementation consisting of a single server that is not part of a multiplex. Contrast with multiplex.

singleton installation – a Sybase Control Center installation that runs a single SCC agent or server. Contrast with instance; see also shared-disk mode.

store – a store is one or more dbspaces that store persistent or temporary data for a special purpose. See catalog store, main store, or temporary store.

table version – the unit of versioning is the table. Table-level versioning structures aggregate data for columns at the table level. With table-level versioning, SAP Sybase IQ can control access to the data at the level where write operations occur, and where query results are focused.

temporary store – the SAP Sybase IQ temporary store is the portion of each SAP Sybase IQ database that stores temporary tables and temporary scratch space data structures. The SAP Sybase IQ server uses temporary data structures to sort and process data. Data in these tables persists only as long as you are connected to the database.

text configuration object – associated with a text index to define the way the index breaks text into terms, or searchable strings. You can create your own text configuration object or use one of the defaults provided by Sybase. See also text index.

text index – a mechanism to speed up full-text searching of tables. You must create a text index for a table before full-text searches can be performed. Each text index requires a text configuration object. See also text configuration object.

topology – a graphical representation of how the servers in a multiplex environment are connected to each other. Found in the IQ Multiplex Level Monitor, it is a network diagram that provides a visual map of the availability of the SAP Sybase IQ server environment.

transaction – a set of related SQL statements that are treated as a single unit of work. To ensure consistency, if all the statements in the set cannot be executed, the changes made by the query are rolled back. The tables queried during the transaction are locked until a transaction is completed.

transaction log – the SAP Sybase IQ transaction log records changes to the database. The transaction log includes version information, free space, and other information you can use to recover from a system failure. By default, the transaction log is created in the same directory as the catalog store. The default name for this dbfile is *<dbname>.log*.

trend period – See chart trend period.

view (SCC) – a window in a Sybase Control Center perspective that displays information about one or more managed resources. Some views also let you interact with managed resources or with SCC itself. For example, the Perspective Resources view lists all the resources managed by the current perspective. Other views allow you to configure alerts, view the topology of a replication environment, and graph performance statistics.

Index

- Xmx maximum memory option 45, 90
- XX:MaxPermSize permanent memory option 45, 90
- .NET external environments, Sybase IQ
 - modifying properties 1230
 - setting location 1230
 - viewing properties 1230

A

- accessibility 15
- Administration Console
 - column filtering 8
 - display tools and options 7
 - displaying only selected resources 321, 322
 - message rows in result sets 322
 - proxy rows 322
 - setting data retrieval thresholds 118
 - using 321
- Adobe Flex 15
- agent, Sybase Control Center
 - See SCC agent
- alert notifications 1347
- alert storm 1347
- alert storm suppression 1347
- alert subscriptions
 - disabling 1301
 - enabling 1301
- alert type 1347
- alert-triggered scripts 303, 1297
 - examples 304
 - substitution parameters 305
- alerts 1347
 - about 1294
 - configured, deleting 1298
 - configured, modifying 1297
 - configured, viewing 1296
 - configuring duplicate alerts 297
 - configuring e-mail server 66, 116
 - configuring escalations 297
 - configuring for SAP Sybase IQ multiplex 298
 - configuring storm suppression 296
 - configuring subscriptions 297
 - configuring to execute scripts 296
 - creating 295
 - displaying history 1301
 - displaying resolutions 1301
 - effects of repository purging on history 1324
 - escalations 1299
 - log 303
 - modifying subscriptions 1299
 - monitoring 1296
 - not being generated 1338
 - notifications, about 1301
 - notifications, viewing 1296
 - resolving 1302
 - SAP Sybase IQ 298
 - script examples 304
 - scripts executed by 303
 - setting triggering states and thresholds 296
 - subscribing to 1299
 - subscriptions 1299
 - substitution parameters for scripts 305
 - testing 1297
 - triggering scripts, about 303
 - types, states, and severities 1295
 - unsubscribing from 1300
- alerts, SAP Sybase IQ
 - types, states, and severities 302
- ALL logging level 1331
- all statistics, SAP Sybase IQ 328
- allocating space
 - dbspace, Sybase IQ 1151
- authenticate 1347
- authenticating
 - Chinese 1340
 - Japanese 1340
 - SCC agents 279
 - SCC with a managed resource 22, 282
- authentication
 - about 47, 97
 - configuring for LDAP 51, 101
 - configuring for UNIX 49, 99
 - configuring for Windows 48, 98
 - troubleshooting for multiplex nodes, SAP Sybase IQ 1343
- authorities, SAP Sybase IQ 823
 - granting 839, 859
- authorities, Sybase IQ
 - revoking 841, 861

Index

- authority-base user
 - force password change 835
- authority-based
 - adding 823
 - creating 823
 - generate DDL 829
 - groups 855
 - groups, adding user to 850
 - groups, database options 853
 - groups, deleting 848
 - users 823, 827, 831
 - users, adding 823
 - users, database options 828
 - users, deleting 826
 - users, generate DDL 829
- authority-based group permissions 223, 862
- authority-based user
 - change login policy 837
 - change password 834
 - unlock account 836
- authority-based user task permissions 220, 842
- authority-based, groups
 - changing to user 849
 - converting a user 849
- authorization 67, 119
- availability 1347
- availability monitoring
 - SAP Sybase IQ 325

B

- background, running SCC or SCC agent in 39, 84
- backups
 - about 1320
 - changing the schedule 1321
 - forcing 1322
 - restoring from 1323
 - scheduling 1320
 - suspending and resuming 1321
- badges, status 6

C

- C ESQL external environments, Sybase IQ
 - modifying properties 1227
 - setting location 1227
 - viewing properties 1227
- C ODBC external environments, Sybase IQ
 - modifying properties 1228

- setting location 1228
- viewing properties 1228
- C/C++
 - aggregate functions in SAP Sybase IQ 1237
 - creating procedures for SAP Sybase IQ 1252
 - creating table UDFs in SAP Sybase IQ 1257
 - creating TPFs in SAP Sybase IQ 1257
 - scalar functions in SAP Sybase IQ 1237
- cache statistics, SAP Sybase IQ 336, 377
- catalog store, SAP Sybase IQ 1347
- chart trend period 1347
 - SAP Sybase IQ, setting 282
- charts, SAP Sybase IQ
 - settings 282
- CHECK conditions
 - Transact-SQL 748
- check constraints 748
 - enforced 748
 - for domains 747
 - Transact-SQL compatibility 748
- Chinese
 - authentication 1340
- client log, viewing 1329
- CLR external environments, Sybase IQ
 - modifying properties 1230
 - setting location 1230
 - viewing properties 1230
- collection repeat interval, SAP Sybase IQ 1347
- collections 1347
- column default
 - not supported 749
- column filtering in SCC 8
- columns
 - sorting by 7
- compatibility
 - referential integrity constraints 749
- compatibility role
 - add membership 1061
 - change administrative rights 1063
 - display grantees 1057
 - display roles granted 1058
 - display system privileges granted 1059
- computed columns
 - not supported 750
- configuration
 - optional 317
- configurations, text
 - See text configuration objects, SAP Sybase IQ

- configuring
 - SAP Sybase IQ for administration 132
 - SAP Sybase IQ for monitoring 20, 128
 - SCC agent connection data 279
 - SCC for Sybase IQ 71, 127
 - Sybase IQ for monitoring 129
- connection statistics, SAP Sybase IQ 330, 374
- connections, SAP Sybase IQ 1348
- console
 - about 1333
 - commands 1333
- constraints in SAP Sybase IQ
 - DDL 573
- conventions, style and syntax 12
- coordinator node
 - server properties 368, 370
- csi_config.xml file 51, 101

D

- data collection jobs
 - adding 283
 - adding schedules 1291
 - creating 283
 - deleting 1290
 - displaying history 1294
 - executing 1289
 - not saving data 283
 - removing schedules 1292
 - resuming 1290
 - stopping 1289
 - suspending 1290
 - viewing schedules 1292
- data collection schedules
 - adding 283
 - modifying 1293
- data collections
 - SAP Sybase IQ 286
 - troubleshooting timeouts 1339
- data retrieval thresholds
 - setting for Administration Console 118
- database task permissions 144, 463
- databases 1348
 - SAP Sybase IQ 451
- databases, SAP Sybase IQ
 - creating 451
 - creating Perl objects 1204
 - installing JAR files 1194
 - installing Perl objects 1206
 - installing PHP objects 1216, 1217
 - updating JAR files 1196, 1197
 - updating Java classes 1192, 1197
 - updating Perl object 1209
 - updating PHP object 1219, 1220
- databases, Sybase IQ
 - installing Java classes 1189
 - modifying properties 457
 - setting options 456
 - updating Java classes 1191
 - updating Perl object 1208
 - viewing properties 457
- db file task permissions 256, 1169
- DB files
 - DDL to add, Sybase IQ 1166
 - deleting, Sybase IQ 1164
 - emptying, Sybase IQ 1165
 - modifying, Sybase IQ 1167
- DB Files
 - managing in SAP Sybase IQ 1161
- dbfiles
 - adding, Sybase IQ 1162
- dbspace
 - grant create permission 1157
- dbspace task permissions 254, 1159
- dbspaces 1348
 - adding dbfiles in Sybase IQ 1162
 - creating, SAP Sybase IQ 1148
 - DDL to create, Sybase IQ 1152
 - deleting, SAP Sybase IQ 1150
 - managing in SAP Sybase IQ 1148
 - modifying, Sybase IQ 1154
 - preallocating space, Sybase IQ 1151
 - read-only, SAP Sybase IQ 1153
- DDL
 - generating for LDAP server configuration
 - object configuration objects 1142
 - generating for SAP Sybase IQ functions 1240
 - generating for SAP Sybase IQ indexes 598, 739
 - generating for SAP Sybase IQ table constraints 573
 - generating for SAP Sybase IQ table triggers 611
 - generating for SAP Sybase IQ tables 484
 - generating for SAP Sybase IQ text indexes 775
 - generating for SAP Sybase IQ view triggers 682
 - generating for Sybase IQ dbfiles 1166

- generating for Sybase IQ dbspaces 1152
- generating for Sybase IQ domains 752
- generating for Sybase IQ event 1178
- generating for Sybase IQ event schedule 1183
- generating for Sybase IQ external login 448
- generating for Sybase IQ groups 854
- generating for Sybase IQ logical server policies 433
- generating for Sybase IQ logical servers 425
- generating for Sybase IQ login mappings 1112
- generating for Sybase IQ materialized views 703
- generating for Sybase IQ procedures 1261
- generating for Sybase IQ remote server 441
- generating for Sybase IQ standalone role 1001
- generating for Sybase IQ text configuration objects 760
- generating for Sybase IQ user-extended role 956
- generating for Sybase IQ users 829, 908
- generating for Sybase IQ views 655
- generating for Sybase IQ web services 1282
- DDL, authority-based
 - generating for Sybase IQ users 829
- DDL, role-based
 - generating for Sybase IQ standalone role 1001
 - generating for Sybase IQ user-extended role 956
 - generating for Sybase IQ users 908
- deadlock details, SAP Sybase IQ 344
- DEBUG logging level 1331
- default values
 - not supported 749
- defined 1347–1351
- Directory Access Server
 - external login 445
- display options in Sybase Control Center 7
- domain task permissions 202, 754
- domains
 - default values 747
- domains in SAP Sybase IQ
 - deleting 751
- domains in Sybase IQ
 - DDL 752
- drivers
 - ODBC, registering 18, 80

E

- e-mail server, configuring for alerts 66, 116
- engine statistics, SAP Sybase IQ 328
- environment variables
 - SCC_MEM_MAX 43–45, 88–90
 - SCC_MEM_PERM 43–45, 88–90
- ERROR logging level 1331
- errors
 - OutOfMemory 1340
 - REJECT_DUPLICATE_RESOURCE_AND_COLLECTION policy 1339
 - timeouts for data collections 1339
- evaluation
 - quick start instructions 17
- event task permissions 258, 1186
- events 1348
 - creating, SAP Sybase IQ 1171
 - DDL for schedule, Sybase IQ 1183
 - DDL, Sybase IQ 1178
 - deleting, Sybase IQ 1174
 - disabling, Sybase IQ 1175
 - enabling, Sybase IQ 1176
 - managing, Sybase IQ 1171
 - modifying properties, Sybase IQ 1179
 - schedule - creating, SAP Sybase IQ 1181
 - schedule - creating, Sybase IQ 1181
 - schedule - DDL, Sybase IQ 1183
 - schedule - deleting, Sybase IQ 1182
 - schedule - modifying, Sybase IQ 1184
 - triggering, Sybase IQ 1177
 - viewing properties, Sybase IQ 1179
- expiration dates for login accounts 125
- external environment java task permissions
 - classes 261, 1202
 - JAR 261, 1202
- external environment task permissions
 - C ESQ 266, 1228, 1230, 1232
 - C ODBC 266, 1228, 1230, 1232
 - CLR (.NET) 266, 1228, 1230, 1232
- external environments, SAP Sybase IQ 1348
 - about 1189
- external login
 - SAP Sybase IQ 445
- External Login, SAP Sybase IQ
 - creating 446
- external login, Sybase IQ
 - managing 445
- External Login, Sybase IQ
 - DDL 448

deleting 447
viewing 449

F

F11 (browser full screen mode toggle) 9
F5 (browser refresh)
 logging out of Sybase Control Center 1338
failover, Sybase IQ
 designating failover node 410
 performing coordinator node failover 411
FATAL logging level 1331
features, new
 Sybase Control Center for SAP Sybase IQ 1
Flash Player 19
foreground, running SCC or SCC agent in 39, 84
full backups 1320
full screen mode 9
function
 grant execute permission 1244
 revoke execute permission 1245
function task permissions 266, 1246
functions, SAP Sybase IQ
 aggregate, creating in external C/C++ 1237
 creating in Transact-SQL 1233
 creating in Watcom SQL 1233
 deleting 1239
 external, creating in Java 1235
 generating DDL 1240
 scalar, creating in external C/C++ 1237
 table UDF, creating in C/C++ 1257
 table UDF, creating in Java 1257
 TPF, creating in C/C++ 1257
 viewing and modifying properties 1241
functions, Sybase IQ
 samples 1232

G

getting started after installing 19
global role administrator 953, 997
 add 954, 999
 remove 955, 1000
glossaries
 SCC for SAP Sybase IQ terms 1347
graphing statistics 320
grid format, using 7
groups 70, 125
 adding login accounts 69, 122

 assigning monitoring and administration roles
 68, 119
 creating 69, 121
 in LDAP, mapping to SCC roles 61, 111
 in OS, mapping to SCC roles 61, 111
 remove login 122
 removing 121
 removing roles 120
 SCC Administrator 61, 111
 sybase 61, 111
groups, authority-based
 database options 853
 generate DDL 854
groups, SAP Sybase IQ 823, 845
 adding to a parent group 850
 adding users to 850
 changing to user 849
 granting authorities to 859
groups, Sybase IQ
 adding 846
 creating 846
 database options 853
 deleting 848
 generate DDL 854
 properties 855
 removing from a parent group 852
 removing users from 852
 revoking authorities from 861

H

heat chart 1348
 customizing columns 23, 319
 display tools and options 7
 displaying 23, 319
 filtering resources displayed 23, 319
 icons 6
 launch icon 5
help command (console) 1333
historical performance monitoring 320
history displays for alerts 1301

I

icons
 for server status 6
 in SCC toolbar 5
 minimize/maximize sections of a view 9

Index

- identity columns
 - compatibility 749
 - supported as default value 749
- in SAP Sybase IQ, defined 1348
- incremental backups 1320
- indexes in SAP Sybase IQ
 - managing 586
 - types 587
- indexes in Sybase IQ, materialized view
 - managing 733
- indexes, text
 - See text indexes, SAP Sybase IQ
- info command (console) 1334
- INFO logging level 1331
- instances 1348
 - about 31, 74, 1314
 - converting 1312
 - deploying 29, 72, 1311
 - deploying and managing 32, 75, 1315
 - file locations 30, 73, 1312
 - refreshing 1312
 - removing 1313
- interfaces files, importing resources from 277
- IQ
 - See SAP Sybase IQ
- IQ server
 - engine statistics 328
- iq_java.sh script 1200
- isolation levels, SAP Sybase IQ 770

J

- Japanese
 - authentication 1340
- JAR files in SAP Sybase IQ
 - deleting 1197
 - installing 1194
 - modifying properties 1193
 - updating 1196
- JAR files in Sybase IQ
 - modifying properties 1198
- Java
 - creating functions for SAP Sybase IQ 1235
 - creating procedures for SAP Sybase IQ 1252
 - creating table UDFs in SAP Sybase IQ 1257
- Java classes in SAP Sybase IQ
 - deleting 1192, 1197
- Java classes in Sybase IQ
 - installing 1189
 - updating 1191

- Java external environments, SAP Sybase IQ
 - classes files, deleting 1192
 - JAR files, deleting 1197
 - JAR files, installing 1194
 - JAR files, modifying properties 1193
 - JAR files, updating 1196
 - Perl object, deleting 1209
 - Perl object, modifying properties 1210
 - PHP object, deleting 1220
 - PHP object, modifying properties 1221
 - PHP object, updating 1219
 - setting up 1194
- Java external environments, Sybase IQ
 - classes, installing 1189
 - classes, updating 1191
 - JAR files, modifying properties 1198
 - modifying properties 1201
 - Perl object, updating 1208
 - setting location 1201
 - setting up 1189
 - testing configuration 1200
 - viewing properties 1201
- Java system properties
 - displaying information about 1334
- jobs 1348
 - modifying collection intervals 1293
 - resuming 1293
 - suspending 1293
- jvmopt memory options for Windows services 43, 45, 88, 90

K

- Kerberos principal 1109
- key performance areas 1348
- key performance indicators 1348
 - getting values from heat chart icons 23, 319
 - in SAP Sybase IQ data collections 286
 - SAP Sybase IQ 307
- keyboard shortcuts 10
- keyboard shortcuts for Adobe Flex 15
- KPAs 1348
- KPIs 1348

L

- layout for Sybase Control Center views 1309
- LDAP
 - configuration properties 52, 102

- configuring authentication 51, 101
 - configuring to authenticate SCC logins 47, 97
- LDAP server configuration object task permissions 252, 1146
- LDAP, SAP Sybase IQ
 - activating server 1138
 - adding 1134
 - creating 1134
 - LDAP server database object 1133
 - LDAP user authentication 1133
 - managing 1133
- LDAP, Sybase IQ
 - DDL 1142
 - deleting 1137
 - modifying 1143
 - refreshing 1140
 - suspending LDAP server 1139
 - validate user 1141
 - viewing 1143
- lock details, SAP Sybase IQ 343
- log4j.properties file 1331
- logging in to Sybase Control Center 46, 95
 - troubleshooting 1337
- logging in to Sybase Control Center - first user 19
- logging levels 1331
- logging out of Sybase Control Center 96
 - unintentionally, using F5 browser refresh 1338
- logical server
 - monitor settings 419
 - overview statistics 416
- logical server policy
 - creating 429
 - user-defined 433
- logical server policy, Sybase IQ
 - deleting 432
 - generate DDL 433
 - properties 434
- logical server statistics, Sybase IQ 417
- logical server, SAP Sybase IQ 379, 419
 - assignment 423
 - creating 420
 - deleting 421
 - node membership 422
- logical server, Sybase IQ
 - generate DDL 425
 - monitor settings 419
 - overview statistics 416
 - properties 426
 - server statistics 417
- logical servers
 - SAP Sybase IQ, registering 21, 130
- login accounts
 - assigning monitoring and administration roles 68, 119
 - authenticating 22, 282
 - creating automatically (UNIX) 49, 99
 - creating automatically (Windows) 48, 98
 - default 123
 - expiration date, imposing 125
 - granting privileges with roles and groups 61, 111
 - modifying 125
 - native SCC, adding 123
 - predefined 70, 125
 - removing 124
 - removing roles 120
 - suspending 125
- login accounts, default
 - about 19
- login mapping task permissions 249, 1114
- login mappings
 - DDL to add, Sybase IQ 1112
- login mappings, SAP Sybase IQ
 - creating 1109
- login mappings, Sybase IQ 1109
 - deleting 1111
- login modules 47, 97
- login policies, SAP Sybase IQ
 - creating 1116, 1121
 - modifying 1127
 - viewing 1127
- login policies, Sybase IQ
 - deleting 1125
 - login policies 1126
 - managing 1116
- login policy task permissions 251, 1132
- login policy, SAP Sybase IQ 423
- login redirection
 - DDL 433
- login session timeout 96
 - setting 67, 117
- logs
 - agent log, viewing 1329
 - alert services 303
 - alert services log, about 1325
 - changing the logging level 1330
 - client log, about 1325

Index

- client log, viewing 1329
- component logs, about 1325
- configuring 1331
- cut and paste from 1327
- filtering 1327
- repository log, about 1325
- repository log, viewing 1329
- SAP Sybase IQ server 1327
- SCC agent 1327
- SCC agent log, about 1325
- script execution log, about 1325
- server logs, about 1325
- server logs, viewing 1329
- Sybase IQ logs, configuring 1326
- Sybase IQ logs, viewing 1326

M

- main store, SAP Sybase IQ 1348
- managed resources 1303, 1349
- managed servers
 - See managed resources
- materialized view
 - grant permissions 727
 - revoke permissions 728
- materialized view in SAP Sybase IQ
 - index task permissions 199, 743
- materialized view in Sybase IQ
 - set clustered index 698
- materialized view index in SAP Sybase IQ
 - creating 734
 - DDL 739
 - deleting 736
 - properties 740
 - rebuilding 737
 - validating 738
- materialized view task permissions 191, 712
- materialized views in SAP Sybase IQ
 - creating 689
- materialized views in Sybase IQ
 - DDL 703
 - deleting 702
 - disabling 701
 - enabling 699
 - managing 687
 - modifying 705
 - recompiling 699
 - refreshing 692
 - truncating 695
 - validating 696

- viewing materialized view data in SQL 691
- memory
 - configuring 43, 88
 - displaying information about 1334
 - warnings at startup 1340
- memory leak 1340
- memory, insufficient 1337
- message levels 1331
- message rows 1348
 - about 118
 - using 322
- minimize/maximize icon 9
- monitor
 - settings, SAP Sybase IQ 346, 378
 - settings, Sybase IQ 419
- monitor settings, SAP Sybase IQ 346, 378
- monitor settings, Sybase IQ 419
- monitoring
 - performance 320
 - troubleshooting for multiplex nodes, SAP Sybase IQ 1343
- multiplex
 - monitor settings 378
- multiplex server statistics, SAP Sybase IQ 372
- multiplex server, SAP Sybase IQ
 - changing host name 400
 - changing port number 400
 - changing server name 400
 - moving database file 400
- multiplex server, Sybase IQ
 - configuring 400
- multiplex, SAP Sybase IQ 1348
 - cache statistics 377
 - connection statistics 374
 - failure of SCC to control 1342
 - managing 379
 - monitor settings 378
 - overview statistics 26, 366
 - server statistics 372
 - topology statistics 368
 - transaction statistics 375
 - troubleshooting authentication 1343
- multiplex, SAP Sybase IQSAP Sybase IQ
 - troubleshooting monitoring 1343
- multiplex, Sybase IQ
 - dbspace statistics 376

N

- network statistics, SAP Sybase IQ 340

- nodes in a chart
 - SAP Sybase IQ, selecting 282
 - SAP Sybase IQ, setting maximum number 282
- nodes, SAP Sybase IQ 1349
 - troubleshooting authentication 1343
 - troubleshooting monitoring 1343
- NULL
 - in columns 748
 - Transact-SQL compatibility 748

O

- ODBC drivers
 - registering 18, 80
- online help
 - resetting 1338
- operating system
 - configuring to authenticate SCC logins 47, 97
- operation statistics, SAP Sybase IQ 339
- OutOfMemory errors, SCC 1340
- overview statistics, SAP Sybase IQ 24, 26, 325, 366
- overview statistics, Sybase IQ logical server 416

P

- page usage, SAP Sybase IQ 341
- parameters for scripts 305
- partitions in SAP Sybase IQ
 - column storage specifications 632
 - deleting 624
 - deleting all 625
 - merging 627
 - moving 630, 635
 - splitting 628
- passencrypt utility 63, 113
- passwords
 - encrypting 63, 113
 - for repository database dba account, changing 91
 - for SCC default login account 19
- performance monitoring 320
 - SAP Sybase IQ 325
- Perl
 - creating procedures for SAP Sybase IQ 1252
- Perl external environment task permissions 262, 1214
- Perl external environments, SAP Sybase IQ
 - modifying properties 1212

- Perl objects, creating 1204
- Perl objects, installing 1206
 - setting location 1212
 - viewing properties 1212
- Perl external environments, Sybase IQ
 - testing configuration 1211, 1222
- Perl object in SAP Sybase IQ
 - deleting 1209
- Perl object in Sybase IQ
 - updating 1208
- Perl objects in SAP Sybase IQ
 - modifying properties 1210
- permission requirements
 - external login 143, 450
 - logical server 139, 427
 - logical server policy 141, 436
 - multiplex 134, 412
 - remote server 142, 444
 - simplex 133, 364
- permissions, SAP Sybase IQ
 - granting for monitoring 20, 128, 129
- Perspective Heat Chart view 23, 319
- Perspective Resources view
 - about 1303, 1306
 - display tools and options 7
 - icons 6
 - show/hide icon 5
- perspectives 1349
 - about 1306
 - adding resources 281, 1304
 - creating 281, 1307
 - removing 1307
 - removing a resource 1304
 - renaming 1307
- PH{ external environment task permissions 264, 1225

PHP

- creating procedures for SAP Sybase IQ 1252
- PHP external environments, SAP Sybase IQ
 - modifying properties 1223
- PHP objects, installing 1216, 1217
 - setting location 1223
 - viewing properties 1223
- PHP object in SAP Sybase IQ
 - deleting 1220
 - modifying properties 1221
 - updating 1219
- pluggable authentication modules for UNIX
 - authentication 49, 99

Index

- port conflicts 1337
- port number
 - changing 400
- ports
 - changing 91
 - configuring 64, 114
 - default 91
 - displaying information about 1334
- postinstallation tasks 19
- procedure
 - grant execute permission 1266
 - revoke create permission 1158
 - revoke execute permission 1267
- procedure task permissions 271, 1268
- procedures, SAP Sybase IQ
 - creating 1252
 - creating remote 1254
 - deleting 1260
 - manage 1251
 - samples 1251
- procedures, Sybase IQ
 - executing 1259
 - generating DDL 1261
 - viewing, modifying properties 1263
- product modules 1349
 - displaying versions 11
- production environment, setting up SCC in 28
- properties
 - domain, Sybase IQ 753
 - for resources, changing 1305
 - functions in SAP Sybase IQ, viewing and modifying 1241
 - login mappings, Sybase IQ 1113
 - procedures in Sybase IQ, executing 1259
 - procedures in Sybase IQ, viewing and modifying 1263
- proxy table
 - add permissions 555
 - remove permissions 555
- proxy tables in SAP Sybase IQ
 - modifying properties 512
 - viewing properties 512
- Q**
- quick start instructions 17
- R**
- referential integrity constraints
 - CASCADE not supported 749
 - compatibility 749
- refresh interval
 - SAP Sybase IQ, setting 282
- registering
 - SAP Sybase IQ logical servers 21, 130
 - SAP Sybase IQ servers 21, 130
 - SCC agents 279
- registration
 - about 1303
- REJECT_DUPLICATE_RESOURCE_AND_COLLECTION policy errors 1339
- Remote procedures, creating in SAP Sybase IQ 1254
- remote server
 - external login 445
 - SAP Sybase IQ 437
- Remote Server
 - SAP Sybase IQ 437
- Remote Server, SAP Sybase IQ
 - creating 437
- remote server, Sybase IQ
 - managing 437
- Remote Server, Sybase IQ
 - DDL 441
 - deleting 440
 - testing connection 439
 - viewing properties 442
- repository 1320, 1349
 - backing up 1322
 - changing backup schedule 1321
 - changing database dba password 91
 - configuring purging 1324
 - restoring from backup 1323
 - scheduling backups 1320
- request statistics, SAP Sybase IQ 339
- resource explorer
 - launch icon 5
- Resource Explorer
 - about 1303
 - display tools and options 7
 - searching in 1306
- resources 1349
 - about 1303
 - adding to a perspective 281, 1304
 - authenticating 22, 282
 - browsing and managing 321
 - changing connection properties 1305
 - changing name 1305
 - displaying availability 23, 319

- filtering by column in Admin Console 7
 - importing in batch 277
 - modifying data collection schedules 1293
 - removing from a perspective 1304
 - SAP Sybase IQ, registering 21, 130
 - searching and filtering in Admin Console 322
 - searching for 1306
 - selecting for display in Admin Console 322
 - unregistering 1303
 - restarts
 - configuring in UNIX 39, 84
 - configuring in Windows 36, 81
 - role
 - grant system privilege 1069
 - grant system role 1041
 - revoke system privilege 1072
 - revoke system role 1042
 - role administrator
 - modify administrative rights 951, 996
 - remove 950, 995
 - role administrators 947, 992
 - role-base user
 - force password change 913
 - role-base user-extended role
 - force password change 962
 - role-based
 - generate DDL 908, 956, 1001
 - standalone role, adding 973
 - standalone role, deleting 975
 - standalone role, generate DDL 1001
 - standalone roles 1002
 - user-extended role, adding 922
 - user-extended role, deleting 925
 - user-extended role, generate DDL 956
 - user-extended roles 958
 - user-extended roles, user options 946
 - users 909
 - users, adding 892
 - users, database options 907
 - users, deleting 895
 - users, generate DDL 908
 - role-based user
 - add role 897
 - change login policy 916
 - change password 912
 - convert to user-extended role 896
 - remove role membership 901
 - revoke system privilege 905
 - unlock account 914
 - role-based user task permissions 228, 917
 - role-based user-extended role
 - change login policy 965
 - change password 960
 - unlock account 963
 - role-based users 129
 - role-based users, Sybase IQ
 - deleting 895
 - role-mapping.xml file 61, 111
 - roles
 - assigning to users and groups 68, 119
 - change administrative rights of members 899
 - delete compatibility roles 1066
 - mapping SCC roles to LDAP or OS groups 61, 111
 - predefined 70, 125
 - product level 67, 119
 - removing 120
 - revoke compatibility role 1065
 - system level 67, 119
 - roles, Sybase IQ 891
 - row retrieval threshold
 - setting for Administration Console 118
 - row-level version, SAP Sybase IQ 1349
 - row-level versioning
 - creating an dbspace 1148
 - creating an RLV-enabled table 466
 - dropping an RLV dbspace 1150
 - row-level versioning, SAP Sybase IQ
 - enable 499
 - merge to IQ main store 493
 - RSSD user name, using to authenticate 22, 282
- ## S
- SAP SAP Sybase IQ
 - LDAP server configuration object 1138
 - SAP Sybase IQ
 - all statistics 328
 - authentication 1340, 1342
 - authorities 823, 839, 841, 859, 861
 - cache statistics 336, 377
 - configuring log settings 1326
 - connection statistics 330, 374
 - connection, remote server 439
 - database 451
 - database, creating 1341
 - database, managing 451
 - database, options 451
 - database, properties 451

- database, troubleshooting 1341
- DB files, deleting 1164
- DB files, emptying 1165
- DB files, generating DDL 1166
- DB Files, managing 1161
- DB files, modifying 1167
- dbfiles, adding 1162
- dbspace, managing 1148
- dbspaces, creating 1148
- dbspaces, deleting 1150
- dbspaces, generating DDL 1152
- dbspaces, modifying 1154
- dbspaces, preallocating space 1151
- dbspaces, read-only 1153
- deadlock details 344
- domain properties 753
- domains, creating 746
- domains, managing 746
- event schedule, creating 1181
- event schedule, deleting 1182
- event schedule, generating DDL 1183
- event schedule, modifying 1184
- events, creating 1171
- events, deleting 1174
- events, disabling 1175
- events, enabling 1176
- events, generating DDL 1178
- events, managing 1171
- events, modifying properties 1179
- events, triggering 1177
- events, viewing properties 1179
- external login 445–449
- failover 379, 409–411
- generate DDL 425, 433, 829, 854, 908, 956, 1001
- groups 823, 845, 855
- groups, adding 846
- groups, adding user to 850
- groups, changing to user 849
- groups, database options 853
- groups, deleting 848
- groups, generate DDL 854
- invalid database definition 1341
- LDAP server configuration object 1133, 1134, 1137, 1139, 1140, 1142, 1143
- lock details 343
- log file 1326
- logical server 379, 419–423, 425, 426, 434
- logical server policy 433
- logical server statistics 417
- login mapping properties 1113
- login mappings, generating DDL 1112
- login policies 1116, 1121, 1125, 1127
- Login policy 423
- login, external 445
- monitor settings 346
- monitoring simplex server 325
- monitoring single node server 325
- multiplex 356, 379, 398, 400, 409
- multiplex dbspace statistics 376
- multiplex server statistics 372
- network statistics 340
- operation statistics 339
- overview statistics 24, 26, 325, 366
- page usage 341
- preallocating space 1151
- procedure, remote 1254
- remote procedure 1254
- remote server 437, 440, 441
- remote server connection 439
- request statistics 339
- role-based users, deleting 895
- secondary server 379, 388, 390–392, 395
- sequence generators 788, 790, 792–794
- server 354, 355, 359, 386, 387, 440, 441
- server, changing configuration 347
- server, remote 437
- server, starting 347
- server, stopping 347
- server, viewing log 347
- server, viewing properties 347
- simplex 356, 398
- simplex dbspace statistics 334
- spatial reference system 802, 803, 805–807, 817
- spatial support 802
- spatial unit of measure 802, 812, 815, 816
- standalone role, generate DDL 1001
- standalone roles 1002
- store I/O statistics 335
- table deadlock details 344
- table lock details 343
- table page usage 341
- table version statistics 337
- topology statistics 368
- transaction statistics 332, 375
- user-extended role, generate DDL 956
- user-extended roles 958

- users 823, 831, 892, 909
- users, adding 823, 892
- users, changing to group 827
- users, database options 828, 907
- users, deleting 826
- users, generate DDL 829, 908
- users, removing from a group 852
- version statistics 337
- versions supported 1
- viewing properties, remote server 442
- viewing properties, server 442
- SAP Sybase IQ, defined 1347
- Save data collected from this job checkbox 284
- SCC Administrator group 61, 111
- SCC agent 1342, 1349
 - deploying and managing instances 32, 75, 1315
 - deploying instances from a shared disk 29, 72, 1311
 - multiplex requirements 1342
 - shared disk restriction for multiplex 1342
 - shared-disk mode 30, 74, 1310
 - starting in UNIX 39, 84
 - starting in UNIX as a service 39, 84
 - starting in Windows 36, 81
 - starting in Windows as a service 36, 81
 - stopping in UNIX 39, 84
 - stopping in Windows 36, 81
- scc command 91
 - using to launch Sybase Control Center 18, 80
- scc_iq_monitor_privileges_setup script 20, 128, 129
- SCC_MEM_MAX 43–45, 88–90, 1340
- SCC_MEM_PERM 43–45, 88–90
- SCC_MONITOR group for SAP Sybase IQ 20, 128, 129
- SCC-enabled login account 1349
- scc.bat 18, 36, 80, 81
- scc.sh 39, 84
- sccadmin account
 - about 19
- sccAdminRole 70, 125
- sccd shell script 39, 84
- sccinstance command 32, 75, 1315
- sccUserRole 70, 125
- scheduler
 - resuming 1293
 - suspending 1293
- schedules 1289, 1349
 - adding to a job 1291
 - creating for a data collection job 283
 - removing from a job 1292
 - viewing 1292
- screen refresh interval
 - Sybase IQ, setting 282
- screen refresh interval, SAP Sybase IQ 1350
- screens
 - maximizing 9
 - maximizing and minimizing sections of a view 9
- scripts
 - alert-triggered 1297
 - alert-triggered, examples 304
 - substitution parameters 305
 - triggered by alerts 303
- secondary node
 - server properties 368, 370
- secondary server, SAP Sybase IQ 379
- secondary server, Sybase IQ
 - adding 392
 - dropping 395
 - excluding 390
 - including 388
 - synchronizing 391
- security 47, 97
 - configuring 46, 96
- security modes
 - authority based 822
 - role based 822
- security providers
 - configuring 47, 97
- sequence generator
 - grant usage permission 797
 - revoke usage permission 798
- sequence generator permissions 213, 799
- sequence generators, Sybase IQ 788
 - adding 788
 - creating 788
 - ddl 793
 - deleting 790
 - modifying 794
 - restarting 792
 - viewing 794
- server
 - administration scripts, SAP Sybase IQ 396
 - administration scripts, Sybase IQ 358

Index

- changing configuration, SAP Sybase IQ 347, 379
- starting, SAP Sybase IQ 347
- stopping, SAP Sybase IQ 347
- viewing properties, SAP Sybase IQ 347
- server log, configuring for Sybase IQ 1326
- server log, viewing for Sybase IQ 1326
- server logs, viewing 1329
- server, SAP Sybase IQ
 - starting 386
 - stopping 387
- server, Sybase IQ
 - agent information 359
 - starting 354
 - stopping 355
 - viewing properties 359
- servers
 - authenticating 22, 282
 - displaying availability 23, 319
 - importing in batch 277
 - modifying data collection schedules 1293
 - SAP Sybase IQ, registering 21, 130
 - searching for 1306
 - unregistering 1303
- services
 - enabling and disabling 91
 - listing 1334
- services, UNIX
 - configuring SCC memory options for 45, 90
 - running SCC or SCC agent as 39, 84
- services, Windows
 - configuring Sybase Control Center memory options for 45, 90
 - running SCC or SCC agent as 36, 81
- severities for alerts 1295
- severities for alerts, SAP Sybase IQ 302
- shared disk restriction for multiplex 1342
- shared-disk mode 1350
 - about 31, 74, 1314
 - enabling and disabling 30, 74, 1310
- shutdown command (console) 1335
- simplex server, SAP Sybase IQ
 - converting to multiplex 356, 398
 - data collections 286
 - monitoring 325
- simplex, SAP Sybase IQ 1350
 - dbspace statistics 334
- single node, SAP Sybase IQ
 - all statistics 328
 - cache statistics 336
 - connection statistics 330
 - data collections 286
 - deadlock details 344
 - engine statistics 328
 - lock details 343
 - monitor settings 346
 - monitoring 325
 - network statistics 340
 - operation statistics 339
 - overview statistics 24, 325
 - page usage 341
 - request statistics 339
 - store I/O statistics 335
 - table deadlock details 344
 - table lock details 343
 - table page usage 341
 - table version statistics 337
 - transaction statistics 332
 - version statistics 337
- singleton installation 1350
- sorting by column 7
- spatial reference system, SAP Sybase IQ 802
- spatial reference system, Sybase IQ
 - adding 803
 - creating 803
 - ddl 806
 - deleting 805
 - modifying 807
 - viewing 807
- spatial support task permissions 216, 819
- spatial support, SAP Sybase IQ 802
- spatial unit of measure, SAP Sybase IQ
 - creating 812
- spatial unit of measure, Sybase IQ
 - ddl 816
 - deleting 815
 - properties 817
- SQL
 - creating procedures for SAP Sybase IQ 1252
 - executing a Sybase IQ procedure 1259
 - executing, SAP Sybase IQ 324
 - modifying for a Sybase IQ procedure 1263
 - modifying for an SAP Sybase IQ function 1241
- SQL Anywhere
 - referential integrity constraints 749
- SQL in SAP Sybase IQ
 - Transact-SQL 1233

- Watcom SQL 1233
- sql.ini files, importing resources from 277
- standalone role
 - add membership 977
 - add role 982
 - change administrative rights 979, 984
 - grant system privilege 988
 - revoke membership 980
 - revoke system privilege 991
 - revoke underlying role 986
- standalone role, role-based
 - deleting 975
 - generate DDL 1001
- standalone role, Sybase IQ
 - generate DDL 1001
- standalone roles, role-based
 - properties 1002
- standalone roles, Sybase IQ
 - properties 1002
- start up
 - automatic, configuring in UNIX 39, 84
 - automatic, configuring in Windows 36, 81
- starting Sybase Control Center 18, 80
- states, SAP Sybase IQ 302
- statistics
 - about 285
 - all, SAP Sybase IQ 328
 - availability 285
 - cache, SAP Sybase IQ 336, 377
 - connection, SAP Sybase IQ 330, 374
 - engine, SAP Sybase IQ 328
 - logical servers, Sybase IQ 417
 - multiplex dbspace, Sybase IQ 376
 - multiplex servers, SAP Sybase IQ 372
 - network, SAP Sybase IQ 340
 - operation, SAP Sybase IQ 339
 - overview, logical server 416
 - overview, SAP Sybase IQ 24, 26, 325, 366
 - performance 285
 - request, SAP Sybase IQ 339
 - SAP Sybase IQ, changing update frequency 282
 - simplex dbspace, SAP Sybase IQ 334
 - store I/O, SAP Sybase IQ 335
 - table version, SAP Sybase IQ 337
 - topology, SAP Sybase IQ 368
 - transaction, SAP Sybase IQ 332, 375
 - version, SAP Sybase IQ 337
- statistics chart
 - displaying data for a longer period 1338
 - effects of repository purging on 1324
 - graphing performance counters 320
 - troubleshooting 1338
- status command (console) 1335
- status icons and badges for resources 6
- stoplists in SAP Sybase IQ 755
- store 1350
- store I/O statistics, SAP Sybase IQ 335
- stored procedures
 - executing, SAP Sybase IQ 324
- storm suppression for alerts 296
- substitution parameters for scripts 305
- Sybase Control Center
 - accessibility 15
 - connecting a browser to 19
 - console commands 1333
 - deploying and managing instances 32, 75, 1315
 - deploying instances from a shared disk 29, 72, 1311
 - display tools and options 7
 - displaying component versions 11
 - failure to start 1337
 - keyboard shortcuts 10
 - log files 1329
 - logging in 46, 95
 - logging out 96
 - logging out unintentionally with F5 1338
 - shared-disk mode 30, 74, 1310
 - starting 18, 80
 - starting in UNIX 39, 84
 - starting in UNIX as a service 39, 84
 - starting in Windows 36, 81
 - starting in Windows as a service 36, 81
 - stopping in UNIX 39, 84
 - stopping in Windows 36, 81
- Sybase Control Center agent 1
 - SAP Sybase IQ 280
 - Sybase IQ, configuring 279
- Sybase Control Center for SAP Sybase IQ 1
 - new features 1
- sybase group 61, 111
- Sybase IQ
 - roles 891
 - system roles 891
 - users 891

Index

- system extended role
 - revoke underlying role 1048
- system privilege
 - change administrative rights 904, 943, 989, 1051, 1071
 - display grantees 1068
- system privileges
 - ACCESS SERVER LS 1089
 - alphabetical listing 1106
 - ALTER ANY INDEX 1081
 - ALTER ANY MATERIALIZED VIEW 1083
 - ALTER ANY OBJECT 1085
 - ALTER ANY OBJECT OWNER 1085
 - ALTER ANY PROCEDURE 1090
 - ALTER ANY SEQUENCE 1093
 - ALTER ANY TABLE 1096
 - ALTER ANY TEXT CONFIGURATION 1099
 - ALTER ANY TRIGGER 1101
 - ALTER ANY VIEW 1105
 - ALTER DATABASE 1074
 - ALTER DATATYPE 1077
 - BACKUP DATABASE 1074
 - by functional area 1074
 - CHANGE PASSWORD 1101
 - CHECKPOINT 1075
 - COMMENT ANY OBJECT 1086
 - CREATE ANY INDEX 1082
 - CREATE ANY MATERIALIZED VIEW 1083
 - CREATE ANY OBJECT 1086
 - CREATE ANY PROCEDURE 1090
 - CREATE ANY SEQUENCE 1094
 - CREATE ANY TABLE 1096
 - CREATE ANY TEXT CONFIGURATION 1099
 - CREATE ANY TRIGGER 1101
 - CREATE ANY VIEW 1105
 - CREATE DATATYPE 1077
 - CREATE EXTERNAL REFERENCE 1079
 - CREATE MATERIALIZED VIEW 1083
 - CREATE MESSAGE 1084
 - CREATE PROCEDURE 1090
 - CREATE PROXY TABLE 1097
 - CREATE TABLE 1097
 - CREATE TEXT CONFIGURATION 1100
 - CREATE VIEW 1105
 - data types 1077
 - database 1074
 - database options 1076
 - dbspaces 1077
 - debugging 1078
 - DEBUGGING 1078
 - DELETE ANY TABLE 1097
 - DROP ANY INDEX 1082
 - DROP ANY MATERIALIZED VIEW 1084
 - DROP ANY OBJECT 1086
 - DROP ANY PROCEDURE 1091
 - DROP ANY SEQUENCE 1094
 - DROP ANY TABLE 1098
 - DROP ANY TEXT CONFIGURATION 1100
 - DROP ANY VIEW 1106
 - DROP CONNECTION 1075
 - DROP DATATYPE 1077
 - DROP MESSAGE 1084
 - events 1078
 - EXECUTE ANY PROCEDURE 1091
 - external environment 1079
 - files 1080
 - indexes 1081
 - INSERT ANY TABLE 1098
 - LDAP 1082
 - LOAD ANY TABLE 1098
 - MANAGE ANY DBSPACE 1078
 - MANAGE ANY EVENT 1079
 - MANAGE ANY EXTERNAL ENVIRONMENT 1079
 - MANAGE ANY EXTERNAL OBJECT 1080
 - MANAGE ANY LDAP SERVER 1082
 - MANAGE ANY LOGIN POLICY 1102
 - MANAGE ANY MIRROR SERVER 1088
 - MANAGE ANY OBJECT PRIVILEGES 1087
 - MANAGE ANY SPATIAL OBJECTS 1095
 - MANAGE ANY STATISTICS 1096
 - MANAGE ANY USER 1102
 - MANAGE ANY WEB SERVICE 1106
 - MANAGE AUDITING 1091
 - MANAGE MULTIPLEX 1089
 - MANAGE PROFILING 1075
 - MANAGE REPLICATION 1091
 - MANAGE ROLES 1092
 - materialized views 1083
 - messages 1084
 - mirror server 1088
 - miscellaneous 1084
 - MONITOR 1075
 - multiplex 1089

- procedures 1089
 - READ CLIENT FILE 1080
 - READ FILE 1080
 - REORGANIZE ANY OBJECT 1088
 - replication 1091
 - roles 1092
 - SELECT ANY TABLE 1098
 - sequences 1093
 - server 1094
 - SERVER OPERATOR 1094
 - SET ANY PUBLIC OPTION 1076
 - SET ANY SECURITY OPTION 1076
 - SET ANY SYSTEM OPTION 1076
 - SET ANY USER DEFINED OPTION 1076
 - SET USER 1102
 - spatial objects 1095
 - statistics 1095
 - tables 1096
 - text configurations 1099
 - triggers 1100
 - TRUNCATE ANY TABLE 1099
 - UPDATE ANY TABLE 1099
 - UPGRADE ROLE 1093
 - USE ANY SEQUENCE 1094
 - users and login management 1101
 - VALIDATE ANY OBJECT 1088
 - views 1105
 - web services 1106
 - WRITE CLIENT FILE 1081
 - WRITE FILE 1081
 - system properties
 - displaying information about 1334
 - system role
 - add role 1043
 - change administrative rights 1045
 - display grantees 1037
 - display roles granted 1038
 - display system privileges granted 1039
 - grant system privilege 1049
 - revoke system privilege 1052
 - system roles, Sybase IQ 891
 - system-wide features
 - configuring 46, 96
 - sysuser, SAP Sybase IQ
 - matching case of user IDs with 282
- T**
- table constraint
 - validate 572
 - table constraints
 - rebuild 571
 - table deadlock details, SAP Sybase IQ 344
 - table index in SAP Sybase IQ
 - creating 589, 590
 - DDL 598
 - deleting 593
 - IQ store (main store) 590
 - IQ system store (catalog store) 589
 - moving 596
 - properties 599
 - rebuilding 594
 - validating 595
 - table lock details, SAP Sybase IQ 343
 - table page usage, SAP Sybase IQ 341
 - table parameterized function procedures, creating in SAP Sybase IQ 1257
 - table partitions in SAP Sybase IQ 617
 - table triggers in SAP Sybase IQ
 - DDL 611
 - modifying 612
 - viewing 612
 - table triggers, SAP Sybase IQ
 - creating 607
 - deleting 610
 - table UDF procedures, creating in SAP Sybase IQ 1257
 - table version statistics, SAP Sybase IQ 337
 - table version, SAP Sybase IQ 1350
 - tables
 - grant permissions 549
 - revoke permissions 551
 - tables in SAP Sybase IQ
 - base table 501
 - base tables 466
 - check constraints 574
 - clustered index 492
 - column check constraint 557
 - column check constraints 568
 - column task permissions 159, 540
 - columns, adding 529
 - columns, deleting 533
 - constraint task permissions 163, 580
 - deleting 483
 - deleting partitions 624
 - enable row-level versioning 499
 - foreign key constraint 560
 - foreign key constraints 569
 - global temporary table 506

Index

- global temporary tables 466, 474
 - hash partitions 618
 - hash-range partitions 622
 - index task permissions 169, 603
 - managing 466
 - merging partitions 627
 - modifying properties 501, 506
 - moving 486
 - moving partitions 630
 - moving table objects 497
 - primary key 489
 - primary key constraints 569
 - proxy tables 466, 479
 - range partitions 620
 - rebuild foreign key constraints 571
 - rebuild primary key constraints 571
 - rebuild unique key constraints 571
 - RLV store 493
 - rows, calculating 495
 - specifying column storage for partitions 632
 - splitting partitions 628
 - table check constraint 564
 - table constraints 568
 - table partition permissions 176, 639
 - task permissions 147, 162, 515, 555
 - trigger task permissions 174, 615
 - triggers 606
 - unique constraint 566
 - unique key constraints 569
 - unpartitioning 625
 - validate foreign key constraints 572
 - validate primary key constraints 572
 - validate unique key constraints 572
 - validating 488
 - viewing partitions 635
 - viewing properties 501, 506, 535
 - viewing table data in SQL 481
 - tables in Sybase IQ
 - DDL 484
 - temporary store, SAP Sybase IQ 1350
 - temporary tables
 - Transact-SQL 750
 - terms
 - SCC for SAP Sybase IQ 1347
 - text configuration objects, SAP Sybase IQ 755, 1350
 - about 766
 - creating 755
 - for more information 755
 - stoplists 755
 - text configuration objects, Sybase IQ
 - deleting 758
 - generating DDL 760
 - modifying properties 761
 - text configuration task permissions 203, 764
 - text conventions 12
 - text index task permissions 206, 781
 - text indexes, SAP Sybase IQ 766, 1350
 - about 766
 - creating 766
 - deleting 769
 - for more information 766
 - generating DDL 775
 - modifying properties 777
 - refreshing 770
 - truncating 773
 - thresholds for data retrieval
 - setting for Administration Console 118
 - timeout
 - errors on data collections 1339
 - setting for login sessions 67, 117
 - toolbar icons 5
 - topology
 - link properties 370
 - topology statistics, SAP Sybase IQ 368
 - topology, SAP Sybase IQ 1350
 - TPF procedures, creating in SAP Sybase IQ 1257
 - Transact-SQL
 - referential integrity constraints 749
 - Transact-SQL functions in SAP Sybase IQ 1233
 - transaction log, SAP Sybase IQ 1350
 - transaction statistics, SAP Sybase IQ 332, 375
 - transactions 1350
 - troubleshooting
 - SAP Sybase IQ 1337
 - types of alerts 1295
 - types of alerts, SAP Sybase IQ 302
- ## U
- ### UNIX
- configuring authentication 49, 99
 - running SCC or SCC agent in the background 39, 84
 - running SCC or SCC agent in the foreground 39, 84
 - starting, stopping SCC or SCC agent 39, 84
- ### user
- grant system privilege 902, 1069

- grant system role 1041
 - revoke system privilege 1072
 - revoke system role 1042
 - user accounts
 - default 123
 - native SCC, adding 123
 - native SCC, not using 47, 97
 - user information
 - modifying 125
 - user interface, about 4
 - user profile
 - Windows 1109
 - user-extended role
 - add compatibility role 933
 - add membership 928
 - add role 933
 - add system role 933
 - change administrative rights 930, 936
 - convert to user 927
 - grant system privilege 941
 - revoke membership 932
 - revoke system privilege 944
 - revoke underlying role 939
 - user-extended role administrator
 - add 949, 993
 - user-extended role, role-based
 - deleting 925
 - generate DDL 956
 - user-extended role, Sybase IQ
 - generate DDL 956
 - user-extended roles, role-based
 - properties 958
 - user-extended roles, Sybase IQ
 - properties 958
 - users, authority-based
 - database options 828
 - deleting 826
 - generate DDL 829
 - properties 831
 - removing from a group 852
 - users, role-based
 - adding 892
 - creating 892
 - database options 907
 - deleting 895
 - generate DDL 908
 - properties 909
 - users, SAP Sybase IQ 823
 - adding to a group 850
 - changing to group 827
 - granting authorities to 839
 - matching case used in sysusers for authentication 282
 - users, Sybase IQ 891, 892
 - adding 823, 892
 - creating 823, 892
 - database options 828, 907
 - deleting 826
 - generate DDL 829, 908
 - properties 831, 909
 - removing from a group 852
 - revoking authorities from 841
- ## V
- version statistics, SAP Sybase IQ 337
 - versions of SCC components
 - displaying 11
 - view
 - grant permissions 672
 - revoke permissions 673
 - view layouts, Sybase Control Center
 - cascade 1309
 - close all 1309
 - horizontal tiling 1309
 - minimize all 1309
 - restore all 1309
 - vertical tiling 1309
 - View menu 9
 - view triggers in SAP Sybase IQ
 - DDL 682
 - modifying 683
 - viewing 683
 - view triggers, SAP Sybase IQ
 - creating 679
 - deleting 681
 - views
 - icons for managing 5
 - maximizing and minimizing sections 9
 - views in SAP Sybase IQ
 - creating 648
 - managing 647
 - trigger task permissions 189, 685
 - views in Sybase IQ
 - DDL 655
 - deleting 653
 - disabling 652
 - enabling 651
 - managing 647

Index

- modifying 656
 - recompiling 651
 - viewing view data in SQL 650
- views task permissions 184, 660
- views, SCC 1351
- views, Sybase Control Center
 - about 1308
 - bringing to front of perspective 1308
 - closing 1308
 - maximizing 1308
 - minimizing 1308
 - opening 1308
 - restoring 1308

W

- WARN logging level 1331
- Watcom SQL functions in SAP Sybase IQ 1233

- Web service task permissions 276, 1286
- web services in Sybase IQ
 - DDL 1282
- web services, SAP Sybase IQ
 - creating 1274
- web services, Sybase IQ 1273
 - deleting 1281
 - disabling 1280
 - enabling 1279
 - modifying properties 1283
 - viewing properties 1283
- Windows
 - configuring authentication 48, 98
 - starting, stopping Sybase Control Center or SCC agent 36, 81
- Windows network server
 - connection 1109