



SAP Control Center for Data Assurance

3.3

DOCUMENT ID: DC01633-01-0330-01

LAST REVISED: February 2014

Copyright © 2014 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 SAP Control Center for Data Assurance	1
New Features in SAP Control Center for Data Assurance	1
User Interface Overview	2
Toolbar Icons	2
Status Icons	3
Common Display Options	4
Keyboard Shortcuts	7
Displaying the Versions of SCC Components	8
Style and Syntax Conventions	9
Accessibility Features	10
SAP Control Center Accessibility Information	11
Get Started	13
Quick Start for an Evaluation	13
Get Started in a Production Environment	19
Launching SAP Control Center	54
Registering the ODBC Driver in Windows	54
Starting and Stopping SAP Control Center in Windows	55
Starting and Stopping SAP Control Center in UNIX	57
Configuring Memory Usage	61
scc Command	64
Logging in to SAP Control Center	68
Logging out of SAP Control Center	69
Setting Up Security	69
Security	70
Configuring Authentication for Windows	71
Configuring a Pluggable Authentication Module (PAM) for UNIX	72
Configuring an LDAP Authentication Module	74

Mapping SAP Control Center Roles to LDAP or OS Groups	84
Encrypting a Password	86
Configuring Ports	87
Configuring the Automatic Logout Timer	89
User Authorization	90
Assigning a Role to a Login or a Group	90
Removing a Role from a Login or a Group	91
Adding a Group	91
Removing a Group	92
Adding a Login Account to a Group	93
Removing a Login Account from a Group	93
Adding a Login Account to the System	94
Removing a Login Account from the System	95
Modifying a User Profile	95
Logins, Roles, and Groups	96
Configure	97
Configuring Data Assurance Server for Monitoring	98
Registering a Data Assurance Server	98
Importing Resources for Batch Registration	99
Authenticating a Login Account for a Managed Resource	100
Setting Up Statistics Collection	101
About Statistics	103
Data Collections for SAP Replication Server	
Data Assurance Option	103
Key Performance Indicators for Data Assurance	104
States for Data Assurance Server, Agents, and Database Connection	104
Creating an Agent Connection	104
Creating a Database Connection	105
Creating a Single or Cluster Connection from an Interface File	107
Optional Configuration Steps	107

Compare Data Rows and Schemas	109
Comparesets	109
Creating a Compareset	109
Editing a Compareset	110
Deleting a Compareset	111
Viewing All Comparesets	111
Viewing Data Partition Boundaries	111
Data Assurance Jobs	112
Row Comparison Jobs	112
Schema Comparison Jobs	119
Manage and Run Data Assurance Jobs	121
Running a Data Assurance Job	121
Deleting a Data Assurance Job	122
Deleting a Comparison in Data Assurance Job ..	122
Viewing All Data Assurance Jobs	122
Viewing a Data Assurance Job Status and Report	123
Data Assurance Job History	123
Manage and Monitor	125
Displaying Resource Availability: the Heat Chart	125
Graphing Performance Counters: the Statistics Chart	126
Manage SAP Control Center	127
Administration Console	127
Job Scheduling	129
Resources	133
Perspectives	136
Views	137
Repository	138
Logging	143
SAP Control Center Console	147
Manage and Monitor the Data Assurance Environment	150
Data Assurance Agents	150
Database Connections	153

Data Assurance Servers	155
Troubleshoot SAP Control Center for Data Assurance ..	159
Comparison Fails to Detect Differences In LOB	
Column	159
External Sort Option Configuration	159
DA Server Out of Memory Errors	160
Problems with Basic SAP Control Center Functionality	
.....	160
SAP Control Center Fails to Start	161
Cannot Log In	161
Browser Refresh (F5) Causes Logout	161
Performance Statistics Do Not Cover Enough	
Time	162
Resetting the Online Help	162
Data Collections Fail to Complete	163
Memory Warnings at Startup	163
SCC Out of Memory Errors	163
Glossary: SAP Control Center for Data Assurance	165
Index	169

About SAP Control Center for Data Assurance

SAP® Control Center for Data Assurance (DA) is a Web-based tool for managing and monitoring the DA server environment.

SAP Control Center for Data Assurance provides availability, historical, and real-time monitoring in a scalable Web application that is integrated with management modules for other SAP 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.

SAP Control Center for Data Assurance supports data comparison from a primary database to one or more replicate databases. The product also supports task scheduling, which allows each comparison task to be run based on a schedule you have specified. It uses and deploys its own SAP® SQL Anywhere® database, which stores system and configuration settings, tasks, and task history. An automatic reconciliation option identifies missing, orphaned, and inconsistent rows when you create DA jobs.

You can monitor servers and agents using the DA monitor, topology view, heat chart, and administration console. History reports for comparison tasks and statistics help you monitor data discrepancies and identify common or recurring problems.

SAP Control Center for Data Assurance is designed to be integrated with SAP® Replication Server® to support comparison of large tables. When you use a SAP Control Center wizard to create a DA job based on a Replication Server system database (RSSD), the wizard is populated automatically with replication definition and subscription information so you can easily create a job with an optimal configuration.

New Features in SAP Control Center for Data Assurance

A brief description for each new and enhanced feature, and links to associated topics.

Table 1. New and Enhanced SAP Control Center for Data Assurance Features

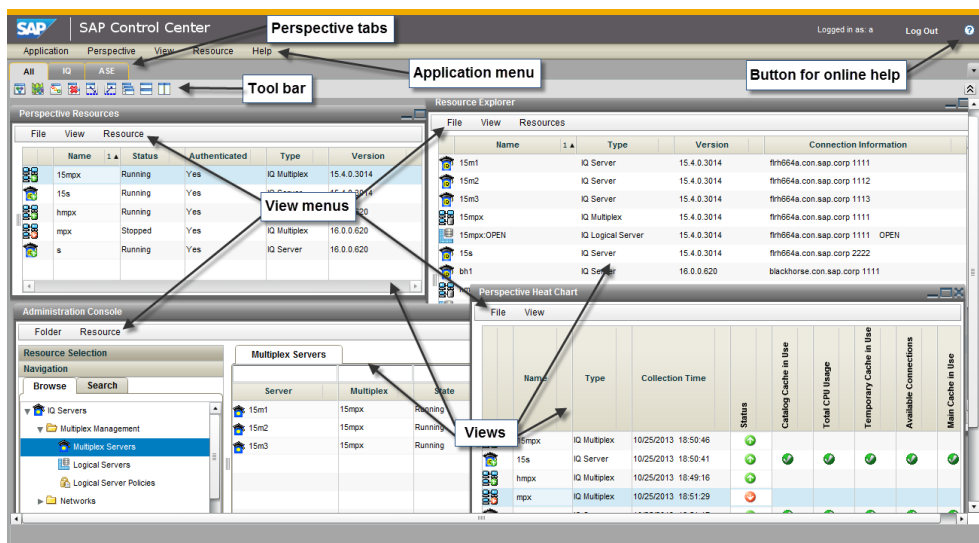
Feature	Topics
<p>New supported database platforms in SCC for Data Assurance version 3.2.8 SP01:</p> <ul style="list-style-type: none"> • Microsoft SQL • IBM DB2 	<p><i>Creating a Database Connection</i> on page 105</p> <p>See the <i>Heterogeneous Comparison</i> in the <i>Replication Server Data Assurance Option Users Guide</i>.</p>

User Interface Overview

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

Tip: Notice that some view menus include options that are similar or identical to options in the application menu (**View** and **Resource**, for example). Although the options have the same names, they have different suboptions. To avoid unexpected results, look for options in the application or view menus as directed in the help.

Figure 1: SAP Control Center User Interface











Toolbar Icons

Describes the icons in the SAP 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.

Icon	Name	Description
	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.

Status Icons


SAP 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




Icon	Status	Description
	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

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 SAP 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.
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). Click any column name to clear the nested sort.
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 SCC 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.

Changing the Font Size

To change the size of fonts in SCC screens:

- Enter **Ctrl-Alt +** to enlarge display fonts.
- Enter **Ctrl-Alt -** to shrink display fonts.

Keyboard Shortcuts

Frequently used key sequences for the SAP 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.

Key Sequence	Action
End	Highlight the last item in the active view (or the active section of a view), for example the last row in a table.
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, Application > Display > Full Screen	Enable or disable SAP Control Center's full-screen mode.

SAP 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.

Displaying the Versions of SCC Components

View a list of components installed in SAP 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 SAP Help Portal at <http://help.sap.com/database>. Look in the documentation set for the product SCC is managing.

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

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
<code>monospaced (fixed-width)</code>	<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
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.

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.

SAP Control Center Accessibility Information

SAP 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 SAP 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>.

Get Started

Set up SAP® Control Center.

Quick Start for an Evaluation

(Optional) Get started using SAP 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 SAP Control Center.

Task

Use these tasks to start SAP 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 SAP Control Center*

Use the scc command to start SAP Control Center.

3. *Getting Started After Installing*

Perform postinstallation testing and configuration.

4. *Registering a Data Assurance Server*

Register a resource (for example, a server that can be monitored) to make SAP Control Center aware of it and its connection information.

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

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

6. *Displaying Resource Availability: the Heat Chart*

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

7. *Viewing Data Assurance Server and Agent Status*

The Data Assurance (DA) monitor shows high-level server and agent information.

See also

- *Get Started in a Production Environment* on page 19

Registering the ODBC Driver in Windows

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

When SAP 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, SCC generates an error and fails to start.

In Windows 2008, Windows 7, and Windows 8, you must use the **Run as administrator** setting to launch SCC 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 SCC for the first time. You need not follow the steps below.

1. In Windows 2008, Windows 7, or Windows 8, 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 SAP Control Center

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

Prerequisites

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

Task

1. Start SAP Control Center.
 - Windows – navigate to `<install_location>\SCC-3_3\bin` and double-click **scc.bat**.
 - UNIX – execute **scc.sh**.

Messages on the progress of the launch appear in a command window. When SAP Control Center is running, the command window becomes the SAP 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 SAP Control Center.

Task

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

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 SCC, direct your browser to:

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

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

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

SCC 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. SAP recommends that you pass authentication responsibility to your operating system or to LDAP, as described in the *Get Started > Setting Up Security* section of the online help.

SAP 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 *SCC-product-name Installation Guide* for instructions.

Registering a Data Assurance Server

Register a resource (for example, a server that can be monitored) to make SAP Control Center aware of it and its connection information.

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

Field	Description
Resource Name	(Required) Name of the resource to register. Enter the actual name of the managed server, using uppercase and lowercase letters. If the name registered in SAP Control Center does not exactly match the server name, some monitoring functions, including the topology view, do not work.
Resource Type	Select a resource type: <ul style="list-style-type: none"> • Data Assurance Server – monitor Data Assurance server.
Description	A brief description to help you identify the resource.

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

Field	Description
Host Name	Local host name
Port Number	Local host port number

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.)
9. Click **Finish**.

Authenticating a Login Account for a Managed Resource

Specify the login account and password SAP 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 SAP 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 SAP 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**.

Note: The **Use my current SCC login** option is not available in SCC for Replication.

5. If you chose **Specify different credentials**, enter the login and password for SAP 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 SAP 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).

Get Started

- 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 Data Assurance Server and Agent Status

The Data Assurance (DA) monitor shows high-level server and agent information.

Prerequisites

- Register and add the server to be monitored to the Perspective Resources view.
- Authenticate the server.

Task

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Monitor**.

Note: You can also view the server status through the status badges on the server icons in the Perspective Resources, Heat Chart, Resource Explorer, and topology views.

Get Started in a Production Environment

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

Prerequisites

Install SAP Control Center and complete the follow-up tasks described in the *SCC-product-name Installation Guide*.

1. *Starting and Stopping SAP Control Center in Windows*

There are several ways to start and stop SAP 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.

2. *Starting and Stopping SAP Control Center in UNIX*

You can start SAP 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.

3. *Configuring Memory Usage*

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

4. *Logging in to SAP Control Center*

Enter the SAP Control Center Web console.

5. *Setting Up Security*

Configure login authentication and map roles.

6. *Configuring the Automatic Logout Timer*

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

7. *User Authorization*

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

8. *Configure*

Configure SAP Control Center for Data Assurance.

Starting and Stopping SAP Control Center in Windows

There are several ways to start and stop SAP 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 SAP Control Center (the server, which includes the management UI) and the SCC 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 always 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 SAP 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 SCC or the SCC agent manually. The command gives you access to the SCC 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 SAP Control Center service for an SCC server or agent.
- Use the **net start** and **net stop** commands. This is another way to run SAP 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 SCC or the SCC agent as a service and configures the service to restart automatically. Before starting, check the Windows Services list for an SAP Control Center service.

Here are the steps for each starting and stopping option:

- **Start SAP Control Center, the SCC agent, or both when they are installed together:**
 - a) (Skip this step for the SCC agent.) If you are starting SAP Control Center for the first time in Windows 2008, Windows 7, or Windows 8, set the **Run as Administrator** option on the command prompt so that SAP 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_3\bin\scc.bat
```

For an instance:

```
%SYBASE%\SCC-3_3\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 SAP 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_3\bin\scc.bat --stop
```

For an instance:

```
%SYBASE%\SCC-3_3\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 "SAP 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 **SAP 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 SAP Control Center service (controlling SAP 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 "SAP control center 3.3"
```

```
The SAP Control Center 3.3 service is starting.....
The SAP Control Center 3.3 service was started
successfully.
```

Get Started

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

```
net start "SAP control center 3.3 (Boston-1) "
```

```
The SAP Control Center 3.3 (Boston-1) service is
starting.....
```

```
The SAP Control Center 3.3 (Boston-1) service was started
successfully.
```

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

For a singleton installation:

```
net stop "SAP control center 3.3"
```

```
The SAP Control Center 3.3 service is stopping.....
```

```
The SAP Control Center 3.3 service was stopped
successfully.
```

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

```
net stop "SAP control center 3.3 (Boston-1) "
```

```
The SAP Control Center 3.3 (Boston-1) service is
stopping.....
```

```
The SAP Control Center 3.3 (Boston-1) service was stopped
successfully.
```

Starting and Stopping SAP Control Center in UNIX

You can start SAP 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 SAP Control Center (the server, which includes the management UI) and the SAP 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 SAP 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 SAP Control Center or the SCC agent manually. You can either:
 - Run **scc.sh** in the foreground to get access to the SCC 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 SCC console.

You can use **scc.sh** to run SAP 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 SCC or the SCC agent automatically.

Here are the steps for each starting and stopping option:

- **Before you start SAP Control Center or the SCC agent for the first time, set environment variables.** Do this only once.

- Change to the parent of the SAP Control Center installation directory. (The parent directory is typically `/opt/sap` or `opt/sybase`.)
- Execute one of the following to set environment variables.

Bourne shell:

```
. SYBASE.sh
```

C shell:

```
source SYBASE.csh
```

- **Run SAP 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 SCC or the SCC agent.

- To start SCC 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_3/bin/scc.sh
```

For an instance:

```
`${SYBASE}/SCC-3_3/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 SAP Control Center or the SCC agent (or both, when they are installed together) in the background.**

You can use **nohup**, **&**, and **>** to run SAP 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 SCC or the SCC agent.

- 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:

Get Started

```
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 SAP 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_3/bin/scc.sh --stop
```

For an instance:

```
$(SYBASE)/SCC-3_3/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 SAP 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 SCC include a shell script, **sccd**, which you can use to configure the SCC service. (Some UNIX platforms supply tools that make service configuration easier; Linux **chkconfig** is an example.)

Note: SAP 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_3/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 SAP Sybase installation (that is, the parent of `SCC-3_3`, the SAP Control Center installation directory). By default, this directory is called `/opt/sybase` if you installed SCC on a machine with an existing Sybase product or environment variable; otherwise the default parent directory is `/opt/sap`.
 - 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 25 or step *5.d* on page 25.
 - 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`

## Get Started

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 SAP Control Center uses, and if so which configuration method to use.

It is not usually necessary to configure memory usage for SAP 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"> <li>• <code>jvmopt=-Xmx</code> – if you are running SAP Control Center as a Windows service</li> <li>• <code>SCC_MEM_MAX</code> – if you are running SCC as a UNIX service</li> <li>• <code>SCC_MEM_MAX</code> – if you are starting SCC from the command line</li> </ul>                | <ul style="list-style-type: none"> <li>• You need to prevent SAP Control Center from using more than a given amount of memory</li> <li>• SAP Control Center fails to start and may display an error: Could not create the Java Virtual machine.</li> <li>• An OutOfMemory error says SAP Control Center is out of heap space</li> <li>• A warning message about system memory appears during the start process</li> <li>• The machine where SAP Control Center is installed has less than 4GB of memory. (Starting SAP Control Center on a machine with less than 4GB of memory triggers the startup warning message about system memory.)</li> </ul> | <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> |
| <p>Permanent memory</p> <ul style="list-style-type: none"> <li>• <code>jvmopt=-XX:MaxPermSize</code> – if you are running SAP Control Center as a Windows service</li> <li>• <code>SCC_MEM_PERM</code> – if you are running SCC as a UNIX service</li> <li>• <code>SCC_MEM_PERM</code> – if you are starting SCC from the command line</li> </ul> | <p>An OutOfMemory error says SAP Control Center is out of permanent generation space</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p>Increase by 32MB increments. If you reach a value equal to twice the default and still see the OutOfMemory error, contact SAP technical support.</p> <p>Default value: 128MB</p>                                                                                     |

You can change memory options in two ways:

- For SAP Control Center started from the command line – execute commands to set one or more environment variables before executing the **scc** command to start SAP 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 SAP Control Center service – modify a file used by the SAP Control Center service. When you use this method, your changes to the memory options persist—SAP Control Center uses them every time it starts as a service.

### See also

- *Logging in to SAP Control Center* on page 29

### **Changing a Memory Option on the Command Line**

Before you start SAP 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 SAP 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 SAP Control Center.

### See also

- *Changing a Memory Option for an SAP Control Center Windows Service* on page 28
- *Changing a Memory Option for an SCC UNIX Service* on page 29

### **Changing a Memory Option for an SAP Control Center Windows Service**

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

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

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

```
<SAP Control Center-install-directory>\SCC-3_3\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 SAP Control Center Windows service.

### See also

- *Changing a Memory Option on the Command Line* on page 28
- *Changing a Memory Option for an SCC UNIX Service* on page 29

### **Changing a Memory Option for an SCC UNIX Service**

To change a memory setting for an SAP 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—SAP Control Center uses them every time it starts as a service.

1. If SAP 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 SAP Control Center UNIX service.

### See also

- *Changing a Memory Option on the Command Line* on page 28
- *Changing a Memory Option for an SAP Control Center Windows Service* on page 28

## **Logging in to SAP Control Center**

Enter the SAP Control Center Web console.

### Prerequisites

Install Adobe Flash Player in the browser you will use for SCC. See the *SCC-product-name Installation Guide*.

### Task

SAP 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 SAP 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 *SCC-product-name Installation Guide*.

---

1. Connect to the SAP 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 26

## Setting Up Security

Configure login authentication and map roles.

Read about security and follow these procedures before you configure SAP 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 13.

---

### 1. *Security*

SAP 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 SAP 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. SAP recommends that you allow SCC to create accounts automatically.

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

Set up SAP 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 SAP Control Center by editing the security configuration file to point to the correct LDAP server.

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

To grant SAP Control Center privileges to users who are authenticated through LDAP or the operating system, associate roles used in SAP 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 SAP Control Center services to new ports.

### See also

- *Configuring the Automatic Logout Timer* on page 49

### **Security**

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

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

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

SAP strongly recommends that you use a common authentication provider for SCC and for SAP database products managed by SCC. A common authentication provider ensures that single sign-on works for users of SAP Control Center and its managed servers.

SCC 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 SCC predefined roles. Authorization is resolved through the mappings between the security module native roles and SCC roles. You can enable mappings by creating a “sybase” group in your operating system or LDAP server and adding all SCC users, or by modifying the `SCC role-mapping.xml` file to configure the mapping of native roles to SCC roles. The security module authenticates the logins and authorizes access to managed resources.

SAP Control Center provides a set of predefined login modules for authentication. All login modules are defined in the `<install_location>/SCC-3_3/conf/csi_config.xml` file. The syntax is defined by the SAP 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

## Get Started

SCC Administrator, which maps to `sccAdminRole`. You can create additional accounts by adding preconfigured user login modules to `csi_config.xml`. However, SAP 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 SCC through an NT Proxy Login module, enter your user name in the format `username@nt-domain-name`. For example, `user@sap`. 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 SCC 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 SCC 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 SAP 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. SAP recommends that you allow SCC to create accounts automatically.

This task is optional. However, if you choose not to create SAP 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 SCC using an account with SCC 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 SCC login accounts, enter each account into SCC manually.

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

### **Configuring a Pluggable Authentication Module (PAM) for UNIX**

Set up SAP 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/<sunos>/pam.conf file (provided with SAP Control Center) to the /etc/pam.conf file on your Solaris platform.                                                                                                                                                                                         |
| Linux    | Copy the <SCC-install-dir>/utility/<linux>/sybase-csi file (provided with SAP Control Center) to the /etc/pam.d directory on your Linux platform.<br><br><b>Note:</b> The sybase-csi file provided with SAP Control Center is not compatible with the most recent SUSE and Red Hat Linux versions. See the examples at the end of this topic for details. |

**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 SAP Control Center) Restart SAP Control Center.
4. (Optional) Change account creation options.
  - a) Log in to SAP 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.

### Examples: PAMs for SUSE Linux 11, Red Hat Enterprise Linux 6.0

For SUSE 11 and later, do not use the `sybase-csi` file provided with SAP 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
```

For Red Hat 6.0 and later, do not use the `sybase-csi` file provided with SAP Control Center. Instead, in your `/etc/pam.d` directory, create a `sybase-csi` file that contains:

```
sybase-csi PAM Configuration (Red Hat style)
auth include system-auth
account include system-auth
password include system-auth
session include system-auth
```

### Next

There are two next steps:

- If you opted not to automatically create SAP Control Center login accounts, enter each account into SAP Control Center manually. SAP 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 SAP Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping SAP Control Center roles to the groups. The group approach is generally more efficient.

### Configuring an LDAP Authentication Module

Configure an LDAP authentication module for SAP 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 SAP recommends), the line that defines it must include `encrypted="true"`. The line should look similar to this:

```

<options name="BindPassword" encrypted="true"
value="1snjikfwregfqr43hu5io..."/>

```

---

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 %SAP_JRE7%\lib\security\cacerts -file
<your cert file and path>
-alias ldapcert -storepass changeit

```

UNIX:

```

keytool -import -keystore $SAP_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 SCC roles to LDAP groups.

**See also**

- *Mapping SAP Control Center Roles to LDAP or OS Groups* on page 44

LDAP Configuration Properties

Use these properties in your `csi_config.xml` file to control the SAP 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"> <li>• <code>sunone5</code> -- SunOne 5.x OR iPlanet 5.x</li> <li>• <code>msad2k</code> -- Microsoft Active Directory, Windows 2000</li> <li>• <code>nsds4</code> -- Netscape Directory Server 4.x</li> <li>• <code>openldap</code> -- OpenLDAP Directory Server 2.x</li> </ul> <p>The value you choose establishes default values for these other authentication properties:</p> <ul style="list-style-type: none"> <li>• RoleFilter</li> <li>• UserRoleMembership</li> <li>• RoleMemberAttributes</li> <li>• AuthenticationFilter</li> <li>• DigestMD5Authentication</li> <li>• UseUserAccountControl</li> </ul> |

| Property          | Default Value        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ProviderURL       | ldap://localhost: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"> <li>• Located on the same machine as your product that is enabled with the common security infrastructure.</li> <li>• Configured to use the default port (389).</li> </ul> <p>Otherwise, use this syntax for setting the value:<br/>ldap://&lt;hostname&gt;:&lt;port&gt;</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 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"> <li>1. dc=&lt;domainname&gt;,dc=&lt;tld&gt;<br/>For example, a machine in the mycompany.com domain would have a search base of dc=mycompany,dc=com.</li> <li>2. o=&lt;company name&gt;,c=&lt;country code&gt;<br/>For example, this might be o=mycompany,c=us for a machine within the Mycompany organization.</li> </ol> <hr/> <p><b>Note:</b> When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> <li>• Do not use special characters, as listed above, in common names or distinguished names in the value of this property.</li> <li>• Do not use Chinese or Japanese characters in user names or passwords of this property.</li> </ul> |
| 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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Property             | Default Value                                                                                                                                                                                                                                                                                                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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"> <li>• simple — For clear-text password authentication.</li> <li>• DIGEST-MD5 — 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.</li> </ul>                                                                                                                   |
| AuthenticationFilter | <p>For most LDAP servers:<br/> <code>(&amp; (uid={uid}) (objectclass=person))</code><br/> or<br/> For Active Directory email lookups: <code>(&amp; (userPrincipalName={uid}) (objectclass=user))</code><br/> <code>[ActiveDirectory]</code><br/> For Active Directory Windows user name lookups: <code>(&amp; (sAMAccountName={uid}) (objectclass=user))</code></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><b>Note:</b> When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> <li>• Do not use special characters, as listed above, in common names or distinguished names in the value of this property.</li> <li>• Do not use Chinese or Japanese characters in user names or passwords of this property.</li> </ul> |

| Property                 | Default Value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AuthenticationScope      | onelevel      | <p>The authentication search scope. The supported values for this are:</p> <ul style="list-style-type: none"> <li>• onellevel</li> <li>• subtree</li> </ul> <p>If you do not specify a value or if you specify an invalid value, the default value is used.</p>                                                                                                                                                                                                                                                                                                                                                                                    |
| AuthenticationSearchBase | None          | <p>The search base used to authenticate users. If this property is not configured, the value for Default-SearchBase is used.</p> <hr/> <p><b>Note:</b> When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> <li>• Do not use special characters, as listed above, in common names or distinguished names in the value of this property.</li> <li>• Do not use Chinese or Japanese characters in user names or passwords of this property.</li> </ul>                                                                                                                                                             |
| 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>SAP recommends that you encrypt passwords, and provides a password encryption utility. If you encrypt BindPassword, include encrypted=true in the line that sets the option. For example:</p> <pre data-bbox="713 579 1180 656">&lt;options name="BindPassword" encrypted="true" value="1snjikf-wregfqr43hu5io..." /&gt;</pre> <p>If you do not encrypt BindPassword, the option might look like this:</p> <pre data-bbox="713 749 1180 800">&lt;options name="BindPassword" value="s3cr3T" /&gt;</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><b>Note:</b> When you use this property to authenticate SCC:</p> <ul data-bbox="713 1034 1185 1190" style="list-style-type: none"> <li>• Do not use special characters, as listed above, in common names or distinguished names in the value of this property.</li> <li>• Do not use Chinese or Japanese characters in user names or passwords of this property.</li> </ul> <hr/>                                                                                                                                                                                                                         |

| Property             | Default Value                                                                                                                                                                                                                                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RoleFilter           | <p>For SunONE/iPlanet:<br/>(<code>&amp;</code>; (object-class=ldapsubentry) (object-class=nsroledefinition))</p> <p>For Netscape Directory Server: ( (object-class=groupofnames) (object-class=groupofunique-names))</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><b>Note:</b> When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> <li>Do not use special characters, as listed above, in common names or distinguished names in the value of this property.</li> <li>Do not use Chinese or Japanese characters in user names or passwords of this property.</li> </ul> |
| RoleMemberAttributes | For Netscape Directory Server and OpenLDAP Server: member,unique-member                                                                                                                                                                                                                                  | <p>A comma-separated list of role attributes from which LDAP derives the DNs 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"> <li>onelevel</li> <li>subtree</li> </ul> <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><b>Note:</b> 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<br>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 <code>temp</code> 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 <code>com.sun.jndi.ldap.connect.timeout</code> 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 <code>com.sun.jndi.ldap.read.timeout</code> 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.<br><br>controlFlag is a generic login module option rather than an LDAP configuration property.                                                                                                                                                                                                                                                                                                                                                                            |

**Mapping SAP Control Center Roles to LDAP or OS Groups**

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

**Prerequisites**

- Required for LDAP and UNIX: Configure an authentication module.
- Optional: Create these groups in the system providing SCC authentication (LDAP or the OS) and assign SAP 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 SAP 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 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          | SAP 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 SAP Control Center is using to authenticate users, and add all users who need to access SAP Control Center to one or both groups.
- Configure SAP 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 SAP 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 SAP Control Center.

### See also

- *Configuring an LDAP Authentication Module* on page 34

### 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 SAP 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 **scs --port** command to assign SAP Control Center services to new ports.

### **Prerequisites**

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

### **Task**

SAP 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 SAP Control Center as described here.

<b>Port Name</b>	<b>Description</b>	<b>Service Names</b>	<b>Property Names</b>	<b>Default Port</b>
db	Database port Present on SCC server	ScsSADataserver 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
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 SAP database products) Present on SCC server and SCC agent	Tds	tdsPort	9998

1. Shut down SAP Control Center.
2. Execute **scc --info ports** to display a list of SAP 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 SAP 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 SAP® SQL Anywhere®, used by the SAP 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.

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

Set the Jini RMI daemon to port 9696.

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

Set the main SAP 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 SAP Control Center. To start SCC, execute a separate **scc** command.

---

## Configuring the Automatic Logout Timer

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

### Prerequisites

Launch SAP 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

- *Setting Up Security* on page 30

## User Authorization

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

Access to SAP Control Center is controlled by login accounts. Permissions assign predefined roles that control tasks the user can perform in SCC, such as administration and monitoring of particular types of servers. The roles can be assigned directly to login accounts or to groups; a

## Get Started

login account inherits the roles of any group to which it belongs. Component product modules assign some roles automatically.

SAP Control Center classifies roles as follows:

- System roles – define how a user can interact with SCC.
- Product roles – define how a user can interact with a particular managed resource in SCC, 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* on page 53

### **Assigning a Role to a Login or a Group**

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

1. From the application menu bar, select **Application > Administration**.
2. In the SAP 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:** SAP 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 51
- *Adding a Login Account to a Group* on page 51
- *Logins, Roles, and Groups* on page 52

**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 SAP 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 50
- *Adding a Login Account to a Group* on page 51
- *Logins, Roles, and Groups* on page 52

**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 SAP 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 50
- *Adding a Group* on page 51
- *Logins, Roles, and Groups* on page 52

**Logins, Roles, and Groups**

SAP Control Center includes predefined login accounts and roles.

A login account identifies a user who can connect to SAP 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.

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

**Table 8. Predefined Login Account**

<b>Login Name</b>	<b>Description</b>
sccadmin	Can use all the administrative features in SAP 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. SCC comes with predefined roles that are intended for use in production environments.

**Table 9. Predefined Roles**

<b>Role</b>	<b>Description</b>
sccUserRole	Provides nonadministrative access to SAP Control Center. Required for all users and assigned automatically to every authenticated user.
sccAdminRole	Provides administrative privileges for managing SAP 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. SCC lets you create groups to suit your business requirements.

**See also**

- *Assigning a Role to a Login or a Group* on page 50

- *Adding a Group* on page 51
- *Adding a Login Account to a Group* on page 51

## **Configure**

Configure SAP Control Center for Data Assurance.

---

**Note:** Before configuring SAP 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 Data Assurance Server for Monitoring*  
Authenticate a Data Assurance (DA) server to monitor using SAP Control Center. When a resource is authenticated, SAP Control Center enables the DA server monitoring option.
2. *Registering a Data Assurance Server*  
Register a resource (for example, a server that can be monitored) to make SAP Control Center aware of it and its connection information.
3. *Importing Resources for Batch Registration*  
(Optional) Import and register multiple servers from an interfaces or sql.ini file.
4. *Authenticating a Login Account for a Managed Resource*  
Specify the login account and password SAP Control Center will use when it connects to your server or agent to collect monitoring data or manage the resource.
5. *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.
6. *Creating an Agent Connection*  
Create a Data Assurance (DA) agent connection required to create comparesets and schema jobs.
7. *Creating a Database Connection*  
Set up a primary and replicate database connection in a Data Assurance (DA) server.
8. *Creating a Single or Cluster Connection from an Interface File*  
Import Data Assurance (DA) resources from an interface file.
9. *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 49
- *Logins, Roles, and Groups* on page 96
- *Setting Up Security* on page 69
- *Assigning a Role to a Login or a Group* on page 90

## Launching SAP Control Center

---

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

### Prerequisites

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

### Task

1. Start SAP Control Center.

- Windows – navigate to `<install_location>\SCC-3_3\bin` and double-click **scc.bat**.
- UNIX – execute **scc.sh**.

Messages on the progress of the launch appear in a command window. When SAP Control Center is running, the command window becomes the SAP 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

- *SAP Control Center Console* on page 147

## Registering the ODBC Driver in Windows

---

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

When SAP 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, SCC generates an error and fails to start.

In Windows 2008, Windows 7, and Windows 8, you must use the **Run as administrator** setting to launch SCC 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 SCC for the first time. You need not follow the steps below.

1. In Windows 2008, Windows 7, or Windows 8, 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**.

## Starting and Stopping SAP Control Center in Windows

There are several ways to start and stop SAP 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 SAP Control Center (the server, which includes the management UI) and the SCC 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 always 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 SAP 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 SCC or the SCC agent manually. The command gives you access to the SCC 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 SAP Control Center service for an SCC server or agent.
- Use the **net start** and **net stop** commands. This is another way to run SAP 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 SCC or the SCC agent as a service and configures the service to restart automatically. Before starting, check the Windows Services list for an SAP Control Center service.

Here are the steps for each starting and stopping option:

- **Start SAP Control Center, the SCC agent, or both when they are installed together:**
  - a) (Skip this step for the SCC agent.) If you are starting SAP Control Center for the first time in Windows 2008, Windows 7, or Windows 8, set the **Run as Administrator**

option on the command prompt so that SAP 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_3\bin\scc.bat
```

For an instance:

```
%SYBASE%\SCC-3_3\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 SAP 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_3\bin\scc.bat --stop
```

For an instance:

```
%SYBASE%\SCC-3_3\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 "SAP 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 **SAP 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 SAP Control Center service (controlling SAP 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 "SAP control center 3.3"

The SAP Control Center 3.3 service is starting.....
The SAP Control Center 3.3 service was started
successfully.
```

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

```
net start "SAP control center 3.3 (Boston-1)"

The SAP Control Center 3.3 (Boston-1) service is
starting.....
The SAP Control Center 3.3 (Boston-1) service was started
successfully.
```

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

For a singleton installation:

```
net stop "SAP control center 3.3"

The SAP Control Center 3.3 service is stopping.....
The SAP Control Center 3.3 service was stopped
successfully.
```

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

```
net stop "SAP control center 3.3 (Boston-1)"

The SAP Control Center 3.3 (Boston-1) service is
stopping.....
The SAP Control Center 3.3 (Boston-1) service was stopped
successfully.
```

## **Starting and Stopping SAP Control Center in UNIX**

You can start SAP 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 SAP Control Center (the server, which includes the management UI) and the SAP 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.

## Get Started

If you start SAP 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 SAP Control Center or the SCC agent manually. You can either:
    - Run **scc.sh** in the foreground to get access to the SCC 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 SCC console.
- You can use **scc.sh** to run SAP 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 SCC or the SCC agent automatically.

Here are the steps for each starting and stopping option:

- **Before you start SAP Control Center or the SCC agent for the first time, set environment variables.** Do this only once.
  - a) Change to the parent of the SAP Control Center installation directory. (The parent directory is typically `/opt/sap` or `opt/sybase.`)
  - b) Execute one of the following to set environment variables.

Bourne shell:

```
. SYBASE.sh
```

C shell:

```
source SYBASE.csh
```

- **Run SAP 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 SCC or the SCC agent.

- a) To start SCC 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_3/bin/scc.sh
```

For an instance:

```
`${SYBASE}/SCC-3_3/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 SAP Control Center or the SCC agent (or both, when they are installed together) in the background.**

You can use **nohup**, **&**, and **>** to run SAP 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 SCC 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 SAP 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_3/bin/scc.sh --stop
```

For an instance:

```
$(SYBASE)/SCC-3_3/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 SAP 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 SCC include a shell script, **sccd**, which you can use to configure the SCC service. (Some UNIX platforms supply tools that make service configuration easier; Linux **chkconfig** is an example.)

---

**Note:** SAP 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_3/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 SAP Sybase installation (that is, the parent of `SCC-3_3`, the SAP Control Center installation directory). By default, this directory is called `/opt/sybase` if you installed SCC on a machine with an existing Sybase product or environment variable; otherwise the default parent directory is `/opt/sap`.
- 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 60 or step 5.d on page 61.
- 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 SAP Control Center uses, and if so which configuration method to use.

It is not usually necessary to configure memory usage for SAP 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"> <li>• <code>jvmopt=-Xmx</code> – if you are running SAP Control Center as a Windows service</li> <li>• <code>SCC_MEM_MAX</code> – if you are running SCC as a UNIX service</li> <li>• <code>SCC_MEM_MAX</code> – if you are starting SCC from the command line</li> </ul>	<ul style="list-style-type: none"> <li>• You need to prevent SAP Control Center from using more than a given amount of memory</li> <li>• SAP Control Center fails to start and may display an error: <code>Could not create the Java Virtual machine.</code></li> <li>• An <code>OutOfMemory</code> error says SAP Control Center is out of heap space</li> <li>• A warning message about system memory appears during the start process</li> <li>• The machine where SAP Control Center is installed has less than 4GB of memory. (Starting SAP Control Center on a machine with less than 4GB of memory triggers the startup warning message about system memory.)</li> </ul>	<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>
<p>Permanent memory</p> <ul style="list-style-type: none"> <li>• <code>jvmopt=-XX:MaxPermSize</code> – if you are running SAP Control Center as a Windows service</li> <li>• <code>SCC_MEM_PERM</code> – if you are running SCC as a UNIX service</li> <li>• <code>SCC_MEM_PERM</code> – if you are starting SCC from the command line</li> </ul>	<p>An <code>OutOfMemory</code> error says SAP Control Center is out of permanent generation space</p>	<p>Increase by 32MB increments. If you reach a value equal to twice the default and still see the <code>OutOfMemory</code> error, contact SAP technical support.</p> <p>Default value: 128MB</p>

You can change memory options in two ways:

- For SAP Control Center started from the command line – execute commands to set one or more environment variables before executing the `scc` command to start SAP 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 SAP Control Center service – modify a file used by the SAP Control Center service. When you use this method, your changes to the memory options persist—SAP Control Center uses them every time it starts as a service.

### **Changing a Memory Option on the Command Line**

Before you start SAP 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 SAP 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 SAP Control Center.

### **See also**

- *Starting and Stopping SAP Control Center in Windows* on page 55
- *Starting and Stopping SAP Control Center in UNIX* on page 57
- *scc Command* on page 64

### **Changing a Memory Option for an SAP Control Center Windows Service**

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

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

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

```
<SAP Control Center-install-directory>\SCC-3_3\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 SAP Control Center Windows service.

### See also

- *Starting and Stopping SAP Control Center in Windows* on page 55

### **Changing a Memory Option for an SCC UNIX Service**

To change a memory setting for an SAP 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—SAP Control Center uses them every time it starts as a service.

1. If SAP 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 SAP Control Center UNIX service.

### See also

- *Starting and Stopping SAP Control Center in UNIX* on page 57

## **scc Command**

Use **scc.bat** (Windows) or **scc.sh** (UNIX) to start and stop SAP 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; SAP 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 SAP 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 SAP Control Center server. This option does not work if you start SCC in the background—the server fails to start if there is no console.
- **-disable** | **--disable** *service-name,service-name...* – disable the specified SAP Control Center services. This option does not work while SAP 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 SCC 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 SAP 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 SAP Control Center.
- **-I** | **--info** [*information-category*] – display the specified categories of information about SAP 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 SCC, 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 SCC 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 SCC, 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 an SCC instance in a shared disk deployment. If you do not enter a name for the instance, it defaults to the host name.

## Get Started

- **-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 SCC uses 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 SAP Control Center and other software on the same system. When you use this option, **scc** does not start SAP 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	ScsSADataserver 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
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	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



Port Name	Description	Service Names	Property Names	Default Port
tds	Tabular Data Stream™ port (used to communicate with other SAP database 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 SCC 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 SCC is running.
- **-stop | --stop** – shut down SCC if it is running.
- **-user | --user [login-name]** – specify the user account SAP Control Center uses 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 SAP Control Center software running on this server. If you use this option, **scc** does not start SAP 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 SCC when the command 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. (The SCC repository is a SQL Anywhere database.)

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

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

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

## Get Started

- **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 SAP Control Center when the command 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

- *Configuring Ports* on page 87
- *Logging or Message Levels* on page 145

## Logging in to SAP Control Center

---

Enter the SAP Control Center Web console.

### Prerequisites

Install Adobe Flash Player in the browser you will use for SCC. See the *SCC-product-name Installation Guide*.

### Task

SAP 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 SAP 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 *SCC-product-name Installation Guide*.

---

1. Connect to the SAP 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`.

---

## Logging out of SAP Control Center

---

When you finish working in SAP 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, SAP 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.
- 

## Setting Up Security

---

Configure login authentication and map roles.

Read about security and follow these procedures before you configure SAP 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 13.

---

### 1. Security

SAP 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 SAP 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. SAP recommends that you allow SCC to create accounts automatically.

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

## Get Started

Set up SAP 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 SAP Control Center by editing the security configuration file to point to the correct LDAP server.

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

To grant SAP Control Center privileges to users who are authenticated through LDAP or the operating system, associate roles used in SAP 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 SAP Control Center services to new ports.

## **Security**

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

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

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

SAP strongly recommends that you use a common authentication provider for SCC and for SAP database products managed by SCC. A common authentication provider ensures that single sign-on works for users of SAP Control Center and its managed servers.

SCC 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 SCC predefined roles. Authorization is resolved through the mappings between the security module native roles and SCC roles. You can enable mappings by creating a “sybase” group in your operating system or LDAP server and adding all SCC users, or by modifying the `SCC role-mapping.xml` file to configure the mapping of native roles to SCC roles. The security module authenticates the logins and authorizes access to managed resources.

SAP Control Center provides a set of predefined login modules for authentication. All login modules are defined in the `<install_location>/SCC-3_3/conf/csi_config.xml` file. The syntax is defined by the SAP 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, SAP 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 SCC through an NT Proxy Login module, enter your user name in the format `username@nt-domain-name`. For example, `user@sap`. 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 SCC 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 SCC 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 SAP 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. SAP recommends that you allow SCC to create accounts automatically.

This task is optional. However, if you choose not to create SAP 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 SCC using an account with SCC 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 SCC login accounts, enter each account into SCC manually.
- Grant privileges to login accounts that require more than basic user access. You can grant privileges by assigning SCC roles directly to the login accounts, or by assigning the login accounts to groups and mapping SCC roles to the groups. The group approach is generally more efficient.

**See also**

- *Mapping SAP Control Center Roles to LDAP or OS Groups* on page 84
- *Adding a Login Account to the System* on page 94

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

Set up SAP 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>&lt;SCC-install-dir&gt;/utility/&lt;sunos&gt;/pam.conf</code> file (provided with SAP Control Center) to the <code>/etc/pam.conf</code> file on your Solaris platform.
Linux	Copy the <code>&lt;SCC-install-dir&gt;/utility/&lt;linux&gt;/sybase-csi</code> file (provided with SAP Control Center) to the <code>/etc/pam.d</code> directory on your Linux platform. <hr/> <b>Note:</b> The <code>sybase-csi</code> file provided with SAP Control Center is not compatible with the most recent SUSE and Red Hat Linux versions. See the examples at the end of this topic for details.

**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 SAP Control Center) Restart SAP Control Center.
4. (Optional) Change account creation options.

- a) Log in to SAP 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.

### Examples: PAMs for SUSE Linux 11, Red Hat Enterprise Linux 6.0

For SUSE 11 and later, do not use the `sybase-csi` file provided with SAP 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
```

For Red Hat 6.0 and later, do not use the `sybase-csi` file provided with SAP Control Center. Instead, in your `/etc/pam.d` directory, create a `sybase-csi` file that contains:

```
sybase-csi PAM Configuration (Red Hat style)
auth include system-auth
account include system-auth
password include system-auth
session include system-auth
```

### Next

There are two next steps:

- If you opted not to automatically create SAP Control Center login accounts, enter each account into SAP Control Center manually. SAP 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 SAP Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping SAP Control Center roles to the groups. The group approach is generally more efficient.

### See also

- *Mapping SAP Control Center Roles to LDAP or OS Groups* on page 84
- *Adding a Login Account to the System* on page 94

## Configuring an LDAP Authentication Module

Configure an LDAP authentication module for SAP 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 SAP 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 %SAP_JRE7%\lib\security\cacerts -file
<your cert file and path>
-alias ldapcert -storepass changeit
```

UNIX:

```
keytool -import -keystore $SAP_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 SCC roles to LDAP groups.

### See also

- *Mapping SAP Control Center Roles to LDAP or OS Groups* on page 84

## LDAP Configuration Properties

Use these properties in your `csi_config.xml` file to control the SAP 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"> <li>• sunone5 -- SunOne 5.x OR iPlanet 5.x</li> <li>• msad2k -- Microsoft Active Directory, Windows 2000</li> <li>• nsds4 -- Netscape Directory Server 4.x</li> <li>• openldap -- OpenLDAP Directory Server 2.x</li> </ul> <p>The value you choose establishes default values for these other authentication properties:</p> <ul style="list-style-type: none"> <li>• RoleFilter</li> <li>• UserRoleMembership</li> <li>• RoleMemberAttributes</li> <li>• AuthenticationFilter</li> <li>• DigestMD5Authentication</li> <li>• UseUserAccountControl</li> </ul>
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"> <li>• Located on the same machine as your product that is enabled with the common security infrastructure.</li> <li>• Configured to use the default port (389).</li> </ul> <p>Otherwise, use this syntax for setting the value:            ldap://&lt;hostname&gt;:&lt;port&gt;</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"> <li>1. <code>dc=&lt;domainname&gt;,dc=&lt;tld&gt;</code> For example, a machine in the mycompany.com domain would have a search base of <code>dc=mycompany,dc=com</code>.</li> <li>2. <code>o=&lt;company name&gt;,c=&lt;country code&gt;</code> For example, this might be <code>o=mycompany,c=us</code> for a machine within the Mycompany organization.</li> </ol> <hr/> <p><b>Note:</b> When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> <li>• Do not use special characters, as listed above, in common names or distinguished names in the value of this property.</li> <li>• Do not use Chinese or Japanese characters in user names or passwords of this property.</li> </ul>
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"> <li>• <code>simple</code> — For clear-text password authentication.</li> <li>• <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.</li> </ul>

Property	Default Value	Description
<p>AuthenticationFilter</p>	<p>For most LDAP servers:            (&amp; (uid={uid}) (objectclass=person))</p> <p>or</p> <p>For Active Directory e-mail lookups: (&amp; (userPrincipalName={uid}) (objectclass=user)) [ActiveDirectory]</p> <p>For Active Directory Windows user name lookups: (&amp; (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><b>Note:</b> When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> <li>• Do not use special characters, as listed above, in common names or distinguished names in the value of this property.</li> <li>• Do not use Chinese or Japanese characters in user names or passwords of this property.</li> </ul>
<p>AuthenticationScope</p>	<p>onelevel</p>	<p>The authentication search scope. The supported values for this are:</p> <ul style="list-style-type: none"> <li>• onellevel</li> <li>• subtree</li> </ul> <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><b>Note:</b> When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> <li>• Do not use special characters, as listed above, in common names or distinguished names in the value of this property.</li> <li>• Do not use Chinese or Japanese characters in user names or passwords of this property.</li> </ul>
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>SAP recommends that you encrypt passwords, and provides a password encryption utility. If you encrypt BindPassword, include encrypted=true in the line that sets the option. For example:</p> <pre data-bbox="713 579 1180 656">&lt;options name="BindPassword" encrypted="true" value="lsnjikf-wregfqr43hu5io..." /&gt;</pre> <p>If you do not encrypt BindPassword, the option might look like this:</p> <pre data-bbox="713 749 1180 800">&lt;options name="BindPassword" value="s3cr3T" /&gt;</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><b>Note:</b> When you use this property to authenticate SCC:</p> <ul data-bbox="713 1034 1185 1190" style="list-style-type: none"> <li>• Do not use special characters, as listed above, in common names or distinguished names in the value of this property.</li> <li>• Do not use Chinese or Japanese characters in user names or passwords of this property.</li> </ul> <hr/>

Property	Default Value	Description
RoleFilter	<p>For SunONE/iPlanet: (<code>&amp;</code>; (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><b>Note:</b> When you use this property to authenticate SCC:</p> <ul style="list-style-type: none"> <li>Do not use special characters, as listed above, in common names or distinguished names in the value of this property.</li> <li>Do not use Chinese or Japanese characters in user names or passwords of this property.</li> </ul>
RoleMemberAttributes	For Netscape Directory Server and OpenLDAP Server: member,unique-member	<p>A comma-separated list of role attributes from which LDAP derives the DNs 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"> <li>onelevel</li> <li>subtree</li> </ul> <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><b>Note:</b> 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 <code>temp</code> 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 <code>com.sun.jndi.ldap.connect.timeout</code> 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 <code>com.sun.jndi.ldap.read.timeout</code> 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 SAP Control Center Roles to LDAP or OS Groups**

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

### **Prerequisites**

- Required for LDAP and UNIX: Configure an authentication module.
- Optional: Create these groups in the system providing SCC authentication (LDAP or the OS) and assign SAP 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 SAP 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 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	SAP 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 SAP Control Center is using to authenticate users, and add all users who need to access SAP Control Center to one or both groups.
- Configure SAP 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 SAP 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 SAP Control Center.

### See also

- *Configuring an LDAP Authentication Module* on page 74

## 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 SAP 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 SAP Control Center services to new ports.

### Prerequisites

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

### Task

SAP 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 SAP 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
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 SAP database products)  Present on SCC server and SCC agent	Tds	tdsPort	9998

1. Shut down SAP Control Center.
2. Execute **scc --info ports** to display a list of SAP 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 SAP 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 SAP® SQL Anywhere®, used by the SAP 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.

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

Set the Jini RMI daemon to port 9696.

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

Set the main SAP 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 SAP Control Center. To start SCC, execute a separate **scc** command.

---

### See also

- *scc Command* on page 64

## Configuring the Automatic Logout Timer

---

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

### Prerequisites

Launch SAP 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 SAP Control Center* on page 54
- *Logging in to SAP Control Center* on page 68

## User Authorization

---

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

Access to SAP Control Center is controlled by login accounts. Permissions assign predefined roles that control tasks the user can perform in SCC, such as administration and monitoring of particular types of 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.

SAP Control Center classifies roles as follows:

- System roles – define how a user can interact with SCC.
- Product roles – define how a user can interact with a particular managed resource in SCC, 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 100

## Assigning a Role to a Login or a Group

---

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

1. From the application menu bar, select **Application > Administration**.
2. In the SAP 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:** SAP 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 91

## Removing a Role from a Login or a Group

Use the security configuration options to remove one or more roles from an SAP 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 SAP 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 90

## 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 SAP 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 92
- *Adding a Login Account to a Group* on page 93
- *Removing a Login Account from a Group* on page 93

## 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 SAP 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 91
- *Adding a Login Account to a Group* on page 93
- *Removing a Login Account from a Group* on page 93

## 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 SAP 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 91
- *Removing a Group* on page 92
- *Removing a Login Account from a Group* on page 93

## 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 SAP 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 91
- *Removing a Group* on page 92
- *Adding a Login Account to a Group* on page 93

## Adding a Login Account to the System

Use the security configuration options to create a native login account in SAP Control Center.

### Prerequisites

- You must have SCC 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:** SAP does not recommend that you manually create a native login account for every SAP Control Center user. It is more efficient to configure SAP 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 SAP 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
  - 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 SAP Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping SAP Control Center roles to the groups. The group approach is generally more efficient.

## **Removing a Login Account from the System**

Use the security configuration options to delete an SAP 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 SAP 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.

## **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 SAP 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 data.
8. Click **Apply**.
9. Click the **User Info** tab.
10. Edit the user information.  
When this user configures e-mail alert subscriptions, SAP Control Center automatically populates the subscription dialog with the e-mail address you enter here.
11. Click **Apply**.

## Logins, Roles, and Groups

SAP Control Center includes predefined login accounts and roles.

A login account identifies a user who can connect to SAP 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.

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

**Table 10. Predefined Login Account**

<b>Login Name</b>	<b>Description</b>
sccadmin	Can use all the administrative features in SAP 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. SCC comes with predefined roles that are intended for use in production environments.

**Table 11. Predefined Roles**

<b>Role</b>	<b>Description</b>
sccUserRole	Provides nonadministrative access to SAP Control Center. Required for all users and assigned automatically to every authenticated user.
sccAdminRole	Provides administrative privileges for managing SAP 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. SCC lets you create groups to suit your business requirements.

# Configure

Configure SAP Control Center for Data Assurance.

---

**Note:** Before configuring SAP 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 Data Assurance Server for Monitoring*  
Authenticate a Data Assurance (DA) server to monitor using SAP Control Center. When a resource is authenticated, SAP Control Center enables the DA server monitoring option.
2. *Registering a Data Assurance Server*  
Register a resource (for example, a server that can be monitored) to make SAP Control Center aware of it and its connection information.
3. *Importing Resources for Batch Registration*  
(Optional) Import and register multiple servers from an interfaces or sql.ini file.
4. *Authenticating a Login Account for a Managed Resource*  
Specify the login account and password SAP Control Center will use when it connects to your server or agent to collect monitoring data or manage the resource.
5. *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.
6. *Creating an Agent Connection*  
Create a Data Assurance (DA) agent connection required to create comparesets and schema jobs.
7. *Creating a Database Connection*  
Set up a primary and replicate database connection in a Data Assurance (DA) server.
8. *Creating a Single or Cluster Connection from an Interface File*  
Import Data Assurance (DA) resources from an interface file.
9. *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 49
- *Logins, Roles, and Groups* on page 96
- *Setting Up Security* on page 69
- *Assigning a Role to a Login or a Group* on page 90

## Configuring Data Assurance Server for Monitoring

---

Authenticate a Data Assurance (DA) server to monitor using SAP Control Center. When a resource is authenticated, SAP Control Center enables the DA server monitoring option.

## Registering a Data Assurance Server

---

Register a resource (for example, a server that can be monitored) to make SAP Control Center aware of it and its connection information.

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

Field	Description
Resource Name	(Required) Name of the resource to register. Enter the actual name of the managed server, using uppercase and lowercase letters. If the name registered in SAP Control Center does not exactly match the server name, some monitoring functions, including the topology view, do not work.
Resource Type	Select a resource type: <ul style="list-style-type: none"> <li>• Data Assurance Server – monitor Data Assurance server.</li> </ul>
Description	A brief description to help you identify the resource.

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

Field	Description
Host Name	Local host name
Port Number	Local host port number

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.)
9. Click **Finish**.

### See also

- *Common Display Options* on page 4
- *Resources* on page 133
- *Unregistering a Resource* on page 133

## 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 SAP database servers and their ports; it may contain other connection information as well. The file is created during the installation of a server:

- 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 SAP Sybase ASE 15.0 *Configuration Guide for Windows*.

---

**Note:** The Import Resources wizard imports servers in batches of a single type (SAP ASE, 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.

## Configure

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, SAP 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 SAP ASE. 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**, SCC 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

- *Resources* on page 133
- *Unregistering a Resource* on page 133

---

## Authenticating a Login Account for a Managed Resource

---

Specify the login account and password SAP 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 SAP 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 SAP 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**.

---

**Note:** The **Use my current SCC login** option is not available in SCC for Replication.

5. If you chose **Specify different credentials**, enter the login and password for SAP 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

- *User Authorization* on page 90

---

## 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.

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 SAP 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**.

## Configure

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. SAP 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 Agent Connection* on page 104
- *Job Scheduling* on page 129
- *Viewing or Deleting a Schedule* on page 132

## **About Statistics**

Understand availability and performance statistics in SAP Control Center.

The statistics you work with in SAP 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.

SAP 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 SAP Control Center:

- Collection repeat interval—The frequency of data collection. Set this on the collection job in the scheduler.
- 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.)

## **Data Collections for SAP Replication Server Data Assurance Option**

Data collection for SAP Control Center for Data Assurance (DA) collects high-level server and agent information.

You may schedule collection of DA data through either a default or predefined data collection. SAP Control Center sets up a default data collection called **collection\_da\_overview** when a DA server is authenticated.

### **See also**

- *Job Scheduling* on page 129

## Key Performance Indicators for Data Assurance

Key performance indicators (KPIs) provide the statistics that appear on Data Assurance (DA) server dashboards and charts in SAP Control Center.

The KPIs used in the Data Assurance default data collection, **collection\_da\_overview** include:

KPI	Description
Server CPU Utilization	The server's overall CPU usage, which is presented in percentages.
Server Memory Utilization	The server's overall memory usage, which is presented in percentages.
Agent CPU Utilization	The agent's overall CPU usage, which is presented in percentages.
Resource State	The state of the resource, which includes Running, Stopped, and Unknown.
Agent Memory Utilization	The agent's overall memory usage, which is presented in percentages.

## States for Data Assurance Server, Agents, and Database Connection

States are used on the dashboards, heat chart, and topology icons.

State	Description
Running	The DA object is in Active state.
Stopped	DA object has been stopped.
Unknown	The state of the DA object cannot be determined.

## Creating an Agent Connection

Create a Data Assurance (DA) agent connection required to create comparesets and schema jobs.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Agent Connections**.
4. Either:
  - Select **Folder > Create Agent Connection**, or,

- Click the button that appears when you select Data Assurance Agent Connections, then select **Create Agent Connection**.

5. Specify the agent connection information:

Field	Description
Data Assurance server	(Required) Name of the DA server from the drop-down list.
Name	(Required) Name of the agent connection. Space is not allowed.
Host	(Required) Name of the server where the DA agent is installed.
Port	(Required) Port number of the DA agent.
Username	(Required) DA agent username.
Password	(Required) DA agent password.
Description	A brief description to help you identify the agent connection.

6. (Optional) Click **Test** to verify if the provided agent connection information is correct.
7. Click **OK**.

The new agent connection profile appears in the Data Assurance Agent Connections table.

### See also

- *Setting Up Statistics Collection* on page 101
- *Data Assurance Agents* on page 150
- *Editing an Agent Connection* on page 151
- *Deleting an Agent Connection* on page 151
- *Viewing All Agent Connection* on page 152
- *Testing an Agent Connection* on page 152

## Creating a Database Connection

---

Set up a primary and replicate database connection in a Data Assurance (DA) server.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Database Connections**.
4. Either:
  - Select **Folder > Create Database Connection**, or,
  - Click the button that appears when you select Database Connections, then select **Create Database Connection**.
5. Specify the database connection information:

## Configure

Field	Description
Data Assurance server	(Required) Name of the DA server from the drop-down list.
Name	(Required) Name of the database connection. Space is not allowed.
Description	A brief description to help you identify the database connection.
Type	(Required) Database type, which includes SAP® Adaptive Server® Enterprise (SAP® ASE), SAP ASE Cluster, Replication Server System Database (RSSD), Oracle, IQ, SAP HANA® database, Microsoft SQL Server, and IBM DB2.
Agent	(Required) The DA agent to use in connecting to the database. It can be a local agent that comes with the DA server installation, a remote agent that is defined in the Data Assurance Agent Connections, or a new remote agent that has yet to be defined.
Database	(Required) Name of the database to connect to.
Host	(Required) Name of the server where the database is residing.
Port	(Required) Port number of the database.
Username	(Required) database username.
Password	Database password.
Properties	The properties for JDBC connection. <b>Note:</b> Enter a number of extra JDBC properties to support SSL connections to SAP ASE.

6. (Optional) Click **Test** to verify if you have specified the correct database information.

7. Click **OK**.

The new database connection appears in the Database Connections table.

### See also

- *Database Connections* on page 153
- *Editing a Database Connection* on page 153
- *Deleting a Database Connection* on page 154
- *Viewing All the Database Connection Profiles* on page 154
- *Testing a Database Connection* on page 154



## Creating a Single or Cluster Connection from an Interface File

---

Import Data Assurance (DA) resources from an interface file.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Database Connections**.
4. Either:
  - Select **Folder > Import Connection**, or,
  - Click the button that appears when you select Database Connections, then select **Import Connection**.
5. Browse through your local drive, select an interface or `sql.ini` file, then click **Next** or **Import Resource Type**.
6. Specify the DA server and resource type to use, then click **Next** or **Resource Selection**.
7. Select the resources to import and the agent that this connection is using, specify the username and password to connect to the selected agent, then click **Next** or **Confirm**.

---

**Note:** The password field is not required.

---

8. Click **Finish**.

### See also

- *Database Connections* on page 153
- *Editing a Database Connection* on page 153
- *Deleting a Database Connection* on page 154
- *Viewing All the Database Connection Profiles* on page 154
- *Testing a Database Connection* on page 154

## Optional Configuration Steps

---

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

**Table 12. Configuration areas**

<b>Configuration area</b>	<b>Description</b>	<b>Topic</b>
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 90
Authentication	Add authentication modules to allow Windows, UNIX, and LDAP users to log in to SAP Control Center.	<i>Setting up Security</i> on page 69
Data collection	Modify collection intervals and schedules, suspend and resume the schedule, and delete collection jobs.	<i>Job Scheduling</i> on page 129
Resources	Unregister resources, add them to perspectives, or remove them.	<i>Resources</i> on page 133
Perspectives	Create, remove, and rename perspectives.	<i>Perspectives</i> on page 136
Repository	Set purging options and schedule backups of the repository database.	<i>Repository</i> on page 138

# Compare Data Rows and Schemas

Compare row data and schema between two or more SAP ASE databases, and view discrepancies.

## Comparesets

---

Comparesets, which consist of sets of tables and columns, define the data being compared in a particular job.

A compareset includes:

- Tables to compare
- Key columns that uniquely define a row
- Columns to compare
- A **WHERE** clause that defines which rows to compare

Source and target tables and columns need not use the same name in a compareset. Each compareset must have one source and one or more targets, and can be used by any number of jobs.

## Creating a Compareset

---

Create a compareset, which includes the database connection profile, and the source and target tables to be compared.

### Prerequisites

Verify that you have created an agent connection.

### Task

1. In the Perspective Resources view, select a Data Assurance server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Comparesets**.
4. Either:
  - Select **Folder > Create Compareset**, or,
  - Click the button that appears when you select Data Assurance Comparesets, then click **Create Compareset**.
5. Specify the compareset basic information, and click **Next** or **Source Table**.

## Compare Data Rows and Schemas

Field	Description
Data Assurance server	(Required) Name of the DA server from the drop-down list.
Name	(Required) Name of the compareset.
Description	A brief description to help you identify the compareset.

6. Select from existing database connections or click **New** to create a new one.
7. Select a schema and a database table.
8. Select the columns to compare.
9. (Optional) Specify constraints to control the comparison job.
10. Click **Next** or **Target Table(s)**.
11. Repeat the same steps performed for the source table.
12. (Optional) Click **Add Target** to define a new target table to compare with the source table.

---

**Note:** You can compare a source table to one or more target table.

---

13. Click **Finish**.

### See also

- *Data Assurance Agents* on page 150
- *Creating an Agent Connection* on page 104
- *Creating a Database Connection* on page 105
- *Creating a Row Comparison Job* on page 112

## Editing a Compareset

Modify the details of an existing compareset.

### Prerequisites

Verify that the compareset you are modifying is not being used in an executing job.

### Task

1. In the Perspective Resources view, select a Data Assurance server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Comparesets**.
4. Select a compareset, then either:
  - Select **Resource > Properties**, or,
  - Click the button that appears when you select a compareset, then select **Properties**.
5. Modify the source and the target tables' details as required.

You also have the option to map the source table to another target table.

6. Click **Apply**, then click **OK**.

### See also

- *Creating a Database Connection* on page 105
- *Creating a Row Comparison Job* on page 112
- *Viewing a Data Assurance Job Status and Report* on page 123

## Deleting a Compareset

Remove a compareset from the list.

### Prerequisites

Verify that the compareset you are deleting is not being used in an executing job.

### Task

1. In the Perspective Resources view, select a Data Assurance server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Comparesets**.
4. Select a compareset, then either:
  - Select **Resource > Delete**, or,
  - Click the button that appears when you select a compareset, then select **Delete**.
5. Click **OK**.

### See also

- *Viewing a Data Assurance Job Status and Report* on page 123

## Viewing All Comparesets

Display all Data Assurance (DA) server comparesets.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Comparesets**.

## Viewing Data Partition Boundaries

Display the data partition boundaries, which Data Assurance stored for each comparesets.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.

## Compare Data Rows and Schemas

3. Expand **Data Assurance Server**, then select **Data Assurance Comparesets**.
4. Select a compareset.
5. Click the button that appears when you select a compareset, then select **Boundaries....**

## Data Assurance Jobs

---

A Data Assurance (DA) job can be a row comparison or a schema comparison.

When creating a row comparison job you specify the compareset to use and set the schedule for running the job. You can set to run a row comparison job based on days, weeks, or months, or you can run it manually. The schema comparison job is run manually and cannot be scheduled.

You can also create a row comparison job based on Replication Server System Database (RSSD) by importing table-level replication definition and subscription from an RSSD in an SAP Replication Server.

See the *Replication Server Data Assurance Option Users Guide > Replication Server Data Assurance Option > Jobs and Comparisons*.

## Row Comparison Jobs

A row comparison sorts rows by a primary or a unique key, from all participating database tables and compares them one by one. A comparison summary is stored in the Data Assurance System Database (DASD). Detailed text or XML reports showing the row differences are stored in the data directory.

In a row job, you create a comparison object, then add a compareset to that particular comparison, set the various comparison parameters, and set the time when the comparison must take place.

### Creating a Row Comparison Job

Set up a row comparison job.

#### **Prerequisites**

Verify that you have created a compareset.

#### **Task**

1. In the Perspective Resources view, select a Data Assurance server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Jobs**.
4. Either:
  - Select **Folder > Create Job**, or,

- Click the button that appears when you select Database Assurance Jobs, then select **Create Job**.

5. Specify the row comparison job basic information:

Field	Description
Data Assurance server	(Required) Name of the DA server from the drop-down list.
Name	(Required) Name of the row comparison job.
Active	Indicates that the row job can be run if selected.
Description	A brief description to help you identify the row comparison job.

6. Click **Next** or **Option**.

7. Enter the value for the maximum concurrent jobs.

This is the maximum number of jobs you want to run at the same time.

8. Click **Next** or **Comparison**.

9. Specify the general information for the current comparison you are setting up.

Field	Description
Name	(Required) Name of the comparison in a row comparison job.
Active	Indicates that the comparison job can be run if selected.
Description	A brief description to help you identify the comparison.
Priority	Priority level for the comparison.
Compareset	Name of the predefined compareset, which has the source and target tables to compare.

**Note:** You can create more than one comparison to a row comparison job, but doing so may result in slow performance. To do this, click **Add Comparison**.

10. (Optional) In the Comparison Options tab, modify or accept the default value for the comparison options.

11. (Optional) In the Column Options tab, modify or accept the default values on the column options for each column from the compareset.

12. (Optional) Click **Next** or **Schedule**.

13. (Optional) Click **With Schedule (s)** to set the schedule for this row comparison job. Or you can set the schedule later or run it manually.

14. Click **Finish**.

**See also**

- *Comparesets* on page 109

### Comparison and Column Options

Be familiar with the comparison and column options provided for creating a row job.

**Table 13. Comparison Options**

Field	Description
Abort condition (rows):	<p>Aborts row comparison if the difference count exceeds the specified value.</p> <p>Valid values: 1 to 9223372036854775807.</p> <p>Default value: 1000.</p>
Abort row count mismatch:	<p>Determines whether to abort row comparison if table row counts do not match.</p> <p>Valid values: true or false.</p> <p>Default value: false.</p>
Auto reconciliation:	<p>Indicates whether to automatically apply the reconciliation script.</p> <p>Valid values: true or false.</p> <p>Default value: false.</p> <hr/> <p><b>Note:</b> To enable <b>AUTO_RECONCILE</b>, set <b>CRE-ATE_COL_LOG</b> to true.</p>
Compare mode:	<p>Specifies the row comparison mode.</p> <ul style="list-style-type: none"> <li>• <code>row_compare</code> – compares all table rows.</li> <li>• <code>key_compare</code> – compares the primary key columns.</li> <li>• <code>row_count</code> – compress row count.</li> </ul> <p>Default value: <code>row_compare</code>.</p>
Compress row data:	<p>Compresses the row data between the agent and the server.</p> <p>Valid values: true or false.</p> <p>Default value: false.</p>



Field	Description
Create column log:	<p>Generates a column differences log, which lists all missing, orphaned, and inconsistent row values (keys and columns). Create a column log if you want to:</p> <ul style="list-style-type: none"> <li>• Generate a reconciliation script</li> <li>• Perform automatic reconciliation</li> <li>• Generate a detailed report</li> </ul> <p>Valid values: true or false. Default value: false.</p>
Create reconciliation script:	<p>Generates a reconciliation script. To use this parameter, you must also set <b>CREATE_COL_LOG</b> to true.</p> <p>Valid values: true or false. Default value: false.</p>
Enable row count:	<p>Determines whether or not to count source and target table rows before they are compared. DA server uses the row count to estimate the comparison progress and end time.</p> <hr/> <p><b>Note:</b> DA server counts rows if <b>COMPARE_MODE</b> is row_count. Use <b>ENABLE_ROW_COUNT</b> only if <b>COMPARE_MODE</b> is a value other than row_count.</p> <hr/> <p>Valid values: true or false. Default value: true.</p>
External sort:	<p>Sorts rows on the agent, thereby reducing the impact of processing the <b>ORDER BY</b> clause in the databases.</p> <p>Valid values: true or false. Default value: false.</p>

## Compare Data Rows and Schemas

Field	Description
Hash type:	<p>Specifies the hash type for the comparison.</p> <ul style="list-style-type: none"> <li>• <code>database_hash</code> – use the hash function provided by the database.</li> <li>• <code>agent_hash</code> – use the hash function provided by Replication Server Data Assurance Option.</li> </ul> <hr/> <p><b>Note:</b> Set the hash type comparison option to <code>agent_hash</code> for heterogeneous comparison. The <code>database_hash</code> comparison option is used only for SAP ASE-to-SAP ASE comparisons.</p>
Maximum retry:	<p>Specifies the total number of recomparison for rows that have differences resulting from a previous comparison.</p> <p>Valid values: 0 to 100.</p> <p>Default value: 3.</p>
Partitions:	<p>Specifies the number of partitions for a table.</p> <hr/> <p><b>Note:</b> This number of partitions needs to be greater than 0 and cannot be set higher than the maximum value of 1024.</p> <hr/> <p>Default value: 1</p>
Retry option:	<p>Specifies the retry option.</p> <ul style="list-style-type: none"> <li>• <code>never</code> – no recompare.</li> <li>• <code>wait_and_retry</code> – run recompare based on <b>RETRY_MAX</b> and <b>RETRY_DELAY_SEC</b> settings.</li> </ul> <p>Default value: never.</p>
Retry delay (seconds):	<p>Specifies the number of seconds delay for each recomparison.</p> <p>Valid values: 0 to 86400.</p> <p>Default value: 10.</p>

**Table 14. Column Comparison Option**

Column Option	Value
Compare mode:	Specifies for how each column is compared. <ul style="list-style-type: none"> <li>• column_hash – compares using column hash value.</li> <li>• row_hash – compares all columns with this option together with a whole hash value.</li> <li>• literal – compares using column literal value.</li> </ul>

**Editing a Row Comparison Job**

Modify details of a Data Assurance (DA) row comparison job.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Job**.
4. Select a row comparison job, then either:
  - Select **Resource > Properties**, or,
  - Click the button that appears when you select a row comparison job, then select **Properties**.
5. Modify the job information on the General, Comparisons, Options, and Schedules tabs as required.

To modify details in Comparisons tab:

- a) Select a comparison, click the button that appears, then select **Properties**.
- b) Modify the comparison information on the General, CompareSet, and Options tabs as required.

Click **Apply** after every modifications in each tab in the Comparisons tab, then click **OK**.

6. Click **Apply**, then click **OK**.

**Scheduling a Row Comparison Job**

Schedule a Data Assurance (DA) row comparison job.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Jobs**.
4. Select a row comparison job, then either:
  - Select **Resource > Properties**, or,

## Compare Data Rows and Schemas

- Click the button that appears when you select a row comparison job, then select **Properties**.
5. Select **Schedules**, click the button that appears, then click **Create Schedule**.
  6. Set the time and day to run this job.
  7. Click **Apply**, then click **OK**.

### **Creating a Job Based on Replication Server System Database**

Create a Data Assurance (DA) job based on an existing table-level replication definition and subscription in a Replication Server.

#### **Prerequisites**

Verify that you have created a Replication Server system database (RSSD) connection.

#### **Task**

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Jobs**.
4. Either:
  - Select **Folder > Import Job from RSSD**, or,
  - Click the button that appears when you select Database Assurance Jobs, then select **Import Job from RSSD**.
5. Specify the job's basic information.

<b>Field</b>	<b>Description</b>
Data Assurance server	(Required) Name of the DA server from the drop-down list.
Name	(Required) Name of the RSSD job.
RSSD connection	(Required) RSSD connection that you want to use, created on the Database Connection.  To choose a Replication Server system database (RSSD) connection, click <b>Select</b> .
Description	A brief description to help you identify the job based on RSSD.
Maximum concurrent jobs	Maximum number of RSSD jobs that you want to run at the same time.
Priority for comparison(s)	Priority level.

6. Click **Next** or **Source DB Mapping**.
7. Select the source database information in RSSD and database connection in DA server.

---

**Note:** The Selected check box filters the comparison generation. Only the replication definition whose primary database argument is in the selected database set will be used to generate a comparison.

---

8. Click **Next** or **Target DB Mapping**.

9. Select the target database information in RSSD and database connection in DA server.

---

**Note:** The Selected check box filters the comparison generation. Only the subscription whose replicate database argument is in the selected database set will be used to generate target argument in the auto-generated comparison.

---

10. Click **Next** or **Comparisons Options**.

11. Specify the comparison options.

12. (Optional) Click **Next** or **Schedule**.

13. Click **Finish**.

### See also

- *Comparison and Column Options* on page 114
- *Creating a Database Connection* on page 105

## Schema Comparison Jobs

Schema comparison lets you compare the schema of one primary database against one or more replicate databases. You can compare an entire database schema using automatic table name mapping, or you can compare specific tables using table name mapping.

### Creating a Schema Comparison Job

Set up a schema comparison job to compare database- and table-level objects in Data Assurance (DA) server.

### Prerequisites

Verify that you have created an agent connection.

### Task

1. In the Perspective Resources view, select a DA server.
2. Select **Resource** > **Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Jobs**.
4. Either:
  - Select **Folder** > **Create Schema Job**, or,
  - Click the button that appears when you select Data Assurance Jobs, then select **Create Schema Job**.

## Compare Data Rows and Schemas

5. Specify the schema job basic and option information.

Field	Description
Data Assurance server	(Required) Name of the DA server from the drop-down list.
Name	(Required) Name of the schema comparison job.
Description	A brief description to help you identify the schema comparison job.
Maximum concurrent jobs	(Required) Maximum number of schema comparison jobs that you want to run at the same time.

6. Click **Next** or **Comparisons**.
7. Click **Create** to specify the comparisons for the schema job.
8. Provide the comparison's basic information.
9. Click **Next** or **Data Sources**.
10. Click **Select Source**.
11. Select a database connection profile for the source data, then click **OK**.
12. Click **Add Target**.

---

**Note:** You can add multiple target databases.

---

13. Select a database connection profile for the target data, then click **OK**.
14. Click **Next** or **Include All Tables**.
15. Select **Include all tables**.
16. (Optional) Click **Add Table** to be excluded from the schema comparison.
17. Click **Next** or **Map Tables**.
18. (Optional) Click **Add Mapping** to specify the source and target table mapping for the schema comparison.

---

**Note:** Set at least one attribute—include-all or table mapping—for one schema comparison. Table mapping allows you to compare schema of tables with different name.

---

19. Click **Finish** twice.

### See also

- *Data Assurance Agents* on page 150
- *Comparison and Column Options* on page 114
- *Deleting a Data Assurance Job* on page 122
- *Running a Data Assurance Job* on page 121
- *Viewing All Data Assurance Jobs* on page 122
- *Viewing a Data Assurance Job Status and Report* on page 123
- *Creating an Agent Connection* on page 104

### **Editing a Schema Comparison Job**

Modify a Data Assurance (DA) schema comparison job details.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Jobs**.
4. Select a schema comparison job, then either:
  - Select **Resource > Properties**, or,
  - Click the button that appears when you select a schema comparison job, then select **Properties**.
5. Modify the schema job information on the General, Comparisons, and Options tabs as required.
 

To modify details in Comparisons tab:

  - a) Select a schema comparison, click the button that appears, then select **Properties**.
  - b) Modify the schema comparison information on the General, Data Source, Include All Tables, and Map Tables tabs as required.

Click **Apply** after every modifications in each tab, then click **OK**.
6. Click **OK**.

#### **See also**

- *Comparison and Column Options* on page 114
- *Deleting a Data Assurance Job* on page 122
- *Running a Data Assurance Job* on page 121
- *Viewing All Data Assurance Jobs* on page 122
- *Viewing a Data Assurance Job Status and Report* on page 123

## **Manage and Run Data Assurance Jobs**

---

Run Data Assurance jobs and view reports, job status and job history.

### **Running a Data Assurance Job**

Run a Data Assurance (DA) row comparison or a schema comparison job.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Jobs**.
4. Select a row or schema comparison job, then either:

## Compare Data Rows and Schemas

- Select **Resource > Run**, or,
- Click the button that appears when you select a row or schema comparison job, then select **Run**.

### Deleting a Data Assurance Job

Remove a Data Assurance (DA) row comparison or a schema comparison job.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Database Assurance Jobs**.
4. Select a row comparison or a schema comparison job, then either:
  - Select **Resource > Delete**, or,
  - Click the button that appears when you select a row comparison or schema comparison job, then select **Delete**.
5. Click **OK**.

### Deleting a Comparison in Data Assurance Job

Delete a comparison in a row or schema comparison job.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Database Assurance Jobs**.
4. Select a row comparison or a schema comparison job, then either:
  - Select **Resource > Properties**, or,
  - Click the button that appears when you select a row comparison or schema comparison job, then select **Properties**.
5. Select **Comparisons**.
6. Select a comparison, click the button that appears, then click **Delete Comparison**.

### Viewing All Data Assurance Jobs

Display a list of all the Data Assurance (DA) row comparison and schema comparison jobs.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Jobs**.



## Viewing a Data Assurance Job Status and Report

Check if a Data Assurance (DA) job is running, pending, finished or aborted, and show report for missing, orphaned, and inconsistent data.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Monitor**.
3. In the Data Assurance Monitor, select **Job Status**.
4. (Optional) Click **Abort** to stop a running job.

## Data Assurance Job History

Data Assurance (DA) job history includes a list of executed jobs with the corresponding time they were submitted and completed.

You can also view a report of these jobs, which you can save as text or XML format.

### Viewing a Job History Report

View the list of completed Data Assurance (DA) jobs, and display their corresponding report.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Select **Data Assurance Job Histories**.
4. Select a DA job, click the button that appears, then select **Report**.

### Deleting a Job History

Remove a job history to clear server space.

1. In the Perspective Resources view, select a Data Assurance (DA) server.
2. Select **Resource > Administration Console**.
3. Select **Data Assurance Job Histories**.
4. Select a DA job, then either:
  - Select **Resource > Delete**, or,
  - Click the button that appears when you select a DA job, then select **Delete**.
5. Click **OK**.

## Compare Data Rows and Schemas

# Manage and Monitor

SAP Control Center allows you to manage and monitor resource availability and view statistics information.

## 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 SAP 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

- *Configuring Repository Purging* on page 142

## Manage SAP Control Center

---

Manage and monitor SAP Control Center for Data Assurance through statistical information and activity logs.

## 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.

---

### **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.

## **Job Scheduling**

A schedule defines a data collection job and specifies how often the job executes in your system.

In SAP 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

## Manage and Monitor

- Date
- Time

The job history displays the status of jobs executed each day.

### **See also**

- *Setting Up Statistics Collection* on page 101
- *Data Collections for SAP Replication Server Data Assurance Option* on page 103

### **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.

### **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.

### **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.

---

### **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. SAP 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**.

### **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**

- *Setting Up Statistics Collection* on page 101

### **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**.

### **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 SAP 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**.

### **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.

## **Resources**

In SAP Control Center, a resource is a unique product component or subcomponent that supports monitoring and management by SCC. A server is the most common managed resource.

Resources you can manage with SCC include servers, agents, databases, devices, and processes. A managed resource is a product component or subcomponent that SCC 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 SCC. The list may include resources that you have not yet added to a perspective. Registration enables SCC 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 makes SCC aware of any manageable subcomponents such as databases or processes. 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 a Data Assurance Server* on page 98
- *Importing Resources for Batch Registration* on page 99

### **Unregistering a Resource**

Remove one or more servers or other resources from SAP Control Center.

1. From the SAP 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

- *Registering a Data Assurance Server* on page 98
- *Importing Resources for Batch Registration* on page 99

### 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 SAP 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 134
- *Resources* on page 133
- *Registering a Data Assurance Server* on page 98
- *Importing Resources for Batch Registration* on page 99

### 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

- *Adding a Resource to a Perspective* on page 134

### Modifying a Resource's Name and Connection Properties

Change the properties of a resource registered with SAP 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 SAP 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).

### 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:

## Manage and Monitor

- **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.

## 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 SAP 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**.

### 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, SAP Control Center displays one.

### 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**.

## Views

Use views to manage one or more resources within a perspective.

In SAP 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:** SAP 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:







<b>Task</b>	<b>Action</b>
Open a view	Do one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• In the application menu bar, select <b>View &gt; Open</b> and choose a view.</li> </ul>
Close a view	Select the view to close. In the application menu bar, select <b>View &gt; Close</b> . You can also click the <b>X</b> 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.

Task	Action
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.
Minimize all views	In the application menu bar, select <b>View &gt; Minimize All Views</b> .
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 <b>View &gt; Select</b> and choose the view you want from the submenu.

### Arranging View Layout in a Perspective

Use the view layout options to manage your perspective space.

Click one of these icons in the SAP Control Center toolbar:

Icon	Action
	<b>Close All Open Views</b>
	<b>Minimize All Open Views</b>
	<b>Restore All Minimized Views</b>
	<b>Cascade All Open Views</b>
	<b>Tile All Open Views Vertically</b>
	<b>Tile All Open Views Horizontally</b>

In a cascade, views overlap; in tiling arrangements, they do not.

Alternatively, you can arrange view layouts from the SAP Control Center menu bar. From the menu bar, select **Perspective > Arrange** and select your view layout.

### Repository

The SAP 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, SAP Control Center saves backups as follows:

- Each full backup is stored in its own subdirectory in `SCC-3_3/backup`.
- Each incremental backup is stored in a file in `SCC-3_3/backup/incremental`.

SAP 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.

### 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.

### 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**.

SAP Control Center saves the backup to the directory shown in the Location field.

### **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 SAP 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 SAP Control Center.
2. Copy the most recent full backup from SCC-3\_3/backup/  
<generated\_directory\_name> to SCC-3\_3/services/Repository. For example:

Windows:

```
copy C:\sap\SCC-3_3\backup\repository.
270110161105\scc_repository.db
C:\sap\SCC-3_3\services\Repository
```

UNIX:

```
cp /opt/sap/SCC-3_3/backup/repository.270110161105/
scc_repository.db
/opt/sap/SCC-3_3/services/Repository
```

3. If you have no incremental backups to load,
  - a) Also copy the log file from SCC-3\_3/backup/  
<generated\_directory\_name> to SCC-3\_3/services/Repository.  
For example:

Windows:

```
copy C:\sap\SCC-3_3\backup\repository.
270110161105\scc_repository.log
C:\sap\SCC-3_3\services\Repository
```

UNIX:

```
cp /opt/sap/SCC-3_3/backup/repository.270110161105/
scc_repository.log
/opt/sap/SCC-3_3/services/Repository
```

- b) Skip to step 5 on page 142.
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 sap\SCC-3_3\services\Repository
```

## Manage and Monitor

```
..\..\bin\sa\bin_<platform>\dbsrv11.exe scc_repository -ad
sap\SCC-3_3\backup\incremental
```

### UNIX:

```
cd /opt/sap/SCC-3_3/services/Repository
```

```
../../bin/sa/bin_<platform>/dbsrv11 scc_repository -ad
/opt/sap/SCC-3_3/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 SAP Control Center.

If you loaded incremental backups, SAP 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:\sap\SCC-3_3\services\Repository
%\bin\sa\bin_windows32\dbsrv11.exe scc_repository -ad
C:\sap\SCC-3_3\backup\incremental
```

These commands start SQL Anywhere on a 64-bit machine running Solaris:

```
$ cd /opt/sap/SCC-3_3/services/Repository
$../../bin/sa/bin_sunsparc64/dbsrv11 scc_repository -ad
/opt/sap/SCC-3_3/backup/incremental
```

### 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 SAP 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 SAP 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**.

## Logging

Logging helps SAP Control Center administrators identify and track errors and other system events by recording messages about the events in log files.

SAP 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 SAP 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 SAP Control Center repository, a SQL Anywhere database. This log is in `SCC-3_3\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_3\log\alert-server.log`.

### **Viewing the Data Assurance Component Log**

View event logs for SAP Control Center for Data Assurance.

The log files are in:

- Windows – %SYBASE%\SCC-3\_3\plugins\DAMAP\log\damap.log
- UNIX – \$SYBASE/SCC-3\_3/plugins/DAMAP/log/damap.log

1. Use a log viewer or text editor to look at log files.
2. Look for entries of interest, such as login attempts or the failure of a service to start.

### **Editing the Data Assurance Log Configuration**

Change the log level or logging configuration settings for Data Assurance (DA).

1. Navigate to %SYBASE%\SCC-3\_2\plugins\DAMAP.
2. Open the `logging.properties` file, and modify the settings as needed.
3. Save and close the `logging.properties` file.
4. Restart the SCC server.

SCC for Data Assurance messages are recorded in the console and the `damap.log` file. The `damap.log` file is located at %SYBASE%\SCC-3\_2\plugins\DAMAP\log.

### **Viewing SAP Control Center Server Logs**

View event logs for the SAP Control Center server.

SAP Control Center logs events to several places:

- The console from which SAP Control Center is launched.
- The SAP 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 SAP 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 SAP Control Center agent log file, some components prepend the component name to log entries.

### **Viewing the SAP Control Center Client Log**

Display the event log for the current session of your SAP 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.

---

### **Changing the Logging Level**

Adjust the logging level that determines which events SAP Control Center records in the server logs. This task requires you to restart SAP Control Center.

If you are having a problem with SAP 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 SAP Control Center.
2. Restart SAP 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 SAP Control Center with the logging level set to debug:

```
Windows: bin\scc -m DEBUG
UNIX: bin/scc -m DEBUG
```

### **See also**

- *Starting and Stopping SAP Control Center in Windows* on page 55
- *Starting and Stopping SAP Control Center in UNIX* on page 57

### **Logging or Message Levels**

Describes values you can use to control the types of events that are logged by SAP 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

- *scc Command* on page 64

### **Changing Logging Configuration**

Edit the logging configuration file, `log4j.properties`, to modify SAP 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 SAP 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 SCC component separately. SAP recommends making such changes only if you are familiar with `log4j` and you are working with SAP 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 SCC.
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"> <li>• Agent log – log4j.appender.agent.File</li> <li>• Repository log – log4j.appender.repository.File</li> <li>• Collection statistics log – log4j.appender.collection-stats.File</li> <li>• Alert server log – log4j.appender.alert.File</li> <li>• Gateway log – log4j.appender.gateway.File</li> </ul>
Change the maximum size that a log file can reach before SCC creates a new file	<ul style="list-style-type: none"> <li>• Agent log – log4j.appender.agent.MaxFileSize</li> <li>• Repository log – log4j.appender.repository.MaxFileSize</li> <li>• Collection statistics log – log4j.appender.collection-stats.MaxFileSize</li> <li>• Alert server log – log4j.appender.alert.MaxFileSize</li> <li>• Gateway log – log4j.appender.gateway.MaxFileSize</li> </ul>
Change the number of log files SCC backs up before deleting the oldest file	<ul style="list-style-type: none"> <li>• Agent log – log4j.appender.agent.MaxBackupIndex</li> <li>• Repository log – log4j.appender.repository.MaxBackupIndex</li> <li>• Collection statistics log – log4j.appender.collection-stats.MaxBackupIndex</li> <li>• Alert server log – log4j.appender.alert.MaxBackupIndex</li> <li>• Gateway log – log4j.appender.gateway.MaxBackupIndex</li> </ul>

5. Save and exit the file.
6. Start SCC to make the logging changes take effect.

### See also

- *Starting and Stopping SAP Control Center in Windows* on page 55
- *Starting and Stopping SAP Control Center in UNIX* on page 57

## SAP Control Center Console

The console is a command-line interface for displaying details about the status of the SAP Control Center server and its subsystems.

When you use the **scc** command to start SAP Control Center, it displays start-up messages and then displays the console prompt.

---

**Note:** The console prompt does not appear if you start SAP Control Center as a service, if you direct the output of **scc** to a file, or if you start SAP Control Center in the background.

---

### See also

- *Launching SAP Control Center* on page 54

### **Console Commands**

Use the SAP Control Center console to get status information on SAP Control Center and its ports, plug-ins, and services.

#### **help Command**

Display syntax information for one or more SAP 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.

#### **info Command**

Display information about specified parts of the SAP 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 SAP 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 SAP 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 SAP 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 SAP 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 SAP Control Center server:

```
info -p
```

### **Permissions**

**info** permission defaults to all users. No permission is required to use it.

### **shutdown command**

Stop the SAP Control Center server if it is running.

### **Syntax**

```
shutdown
```

### **Examples**

- **Example 1** – shuts down SAP Control Center:

```
shutdown
```

### **Permissions**

**shutdown** permission defaults to all users. No permission is required to use it.

### status Command

Display the status of the SAP Control Center agent, plug-in, or service components of SAP Control Center.

### Syntax

```
status [-a | --agent]
[-h | --help]
[-p | --plugin [plugin-name]]
[-s | --service [service-name]]
```

### Parameters

- **-a | --agent** – display the status of the SAP Control Center agent component.
- **-h | --help** – display information about the **info** command.
- **-p | --plugin *[plugin-name]*** – display the status of the specified SAP 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 SAP 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.

## Manage and Monitor the Data Assurance Environment

Manage and monitor Data Assurance server and agents.

### Data Assurance Agents

Data Assurance (DA) agents fetch and compress data from databases into the DA server.

There are two types of agents: the embedded local agent in DA server, and standalone (remote) agents, which DA server can use to improve job performance.

A DA agent opens a Java Database Connectivity (JDBC) connection to one or more databases, and reads the row data used for comparison. If there are no standalone DA agents, you must use the embedded local agent.

Based on the DA server request, a DA agent:

- Compresses rows for precomparison, if configured to do so
- Fetches rows for comparison
- Hashes rows for precomparison, if configured to do so
- Sorts rows for precomparison, if configured to do so
- Runs **insert/delete/update** statements on databases, if configured to do so

### **Editing an Agent Connection**

Modify the details of a Data Assurance (DA) agent connection profile.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Agent Connections**.
4. Select a DA agent connection.
5. Either:
  - Select **Resource > Properties**, or,
  - Click the button that appears when you select a DA agent connection, then select **Properties**.
6. Modify the agent connection information as required, then click **Apply**.

Field	Description
Host	(Required) Name of the server where the DA agent is installed.
Port	(Required) Port number of the DA agent.
Username	(Required) DA agent username.
Password	(Required) DA agent password.
Description	A brief description to help you identify the agent connection.

7. (Optional) Click **Test** to verify if the modified agent connection information is correct.
8. Click **OK**.

### **See also**

- *Creating an Agent Connection* on page 104

### **Deleting an Agent Connection**

Remove a Data Assurance (DA) agent connection profile.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Agent Connections**.

## Manage and Monitor

4. Select a DA agent connection.
5. Either:
  - Select **Resource > Delete**, or,
  - Click the button that appears when you select a DA agent connection, then select **Delete**.
6. Click **OK**.

### See also

- *Creating an Agent Connection* on page 104

### Viewing All Agent Connection

Display the connection profiles of all the Data Assurance (DA) agents.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Agent Connections**.

### See also

- *Creating an Agent Connection* on page 104

### Testing an Agent Connection

Verify that you have properly configured a Data Assurance (DA) agent connection.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Data Assurance Agent Connections**.
4. Select a DA agent connection.
5. Either:
  - Select **Resource > Properties**, or,
  - Click the button that appears when you select a DA agent connection, then select **Properties**.
6. Click **Test**.

### See also

- *Creating an Agent Connection* on page 104

## Database Connections

In SAP Control Center for Data Assurance, you need to create a database connection profile, which contains the information required to establish a database connection to allow comparison of data data between the primary and replicate databases.

### See also

- *Creating a Database Connection* on page 105
- *Creating a Single or Cluster Connection from an Interface File* on page 107

### Editing a Database Connection

Modify the details of a database connection in a Data Assurance (DA) server.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Database Connections**.
4. Select a database connection, then either:
  - Select **Resource > Properties**, or,
  - Click the button that appears when you select a database connection, then select **Properties**.
5. Modify the database connection information as required, then click **Apply**.

Field	Description
Description	A brief description to help you identify the database connection.
Agent	(Required) The DA agent to use in connecting to the database. It can be a local agent that comes with the DA server installation, a remote agent that is defined in the Data Assurance Agent Connections, or a new remote agent that has yet to be defined.
Database	(Required) Name of the database to connect to.
Host	(Required) Name of the server where the database is residing.
Port	(Required) Port number of the database.
Username	(Required) database username.
Password	Database password.
Properties	The properties for JDBC connection.

6. (Optional) Click **Test** to verify if the modified database connection information is correct.
7. Click **OK**.

### See also

- *Creating a Database Connection* on page 105
- *Creating a Single or Cluster Connection from an Interface File* on page 107

### Deleting a Database Connection

Remove a database connection from the Data Assurance (DA) server.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Database Connections**.
4. Select a database connection, then either:
  - Select **Resource > Delete**, or,
  - Click the button that appears when you select a database connection, then select **Delete**.
5. Click **OK**.

### See also

- *Creating a Database Connection* on page 105
- *Creating a Single or Cluster Connection from an Interface File* on page 107

### Viewing All the Database Connection Profiles

Display all the database connection profiles in a Data Assurance (DA) server.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Database Connections**.

### See also

- *Creating a Database Connection* on page 105
- *Creating a Single or Cluster Connection from an Interface File* on page 107

### Testing a Database Connection

Verify that you have properly configured a database connection.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. Expand **Data Assurance Server**, then select **Database Connections**.
4. Select a database connection, then either:
  - Select **Resource > Properties**, or,



- Click the button that appears when you select a database connection, then select **Properties**.

5. Click **Test**.

### See also

- *Creating a Database Connection* on page 105
- *Creating a Single or Cluster Connection from an Interface File* on page 107

## Data Assurance Servers

Gather usage statistics—CPU, memory and cache memory to monitor the availability and state of Data Assurance (DA) servers and agents.

You can monitor the availability and state of objects using the topology and the DA monitor. The topology is a graphical representation of the DA system objects, which include the DA server, agents, and databases.

The monitor includes these views:

- **Overview** – displays high-level information, such as the server name, version number of the server, the server time at last refresh, server status, and memory and CPU usage displayed through chart. You can select to monitor or shutdown a DA server or DA agents using this view.
- **Job Current Status** – displays a list of jobs with their status and other related information, and a list of comparisons, both in a table form. You can choose to abort existing jobs using this view.
- **Settings** – lets you to change the value for the screen refresh interval.

### See also

- *Authenticating a Login Account for a Managed Resource* on page 100

### Displaying the System Topology

The Data Assurance (DA) system topology graphically monitors the DA server and agent availability.

### Prerequisites

- Add the server to be monitored to the Perspective Resources view.
- Authenticate the server.

### Task

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Topology**.

## Manage and Monitor

The topology view opens, displaying the selected DA server and its associated agents and databases.

3. (Optional) Use the View Controls and Details tabs for additional help in viewing the topology.

### **Viewing Data Assurance Server and Agent Status**

The Data Assurance (DA) monitor shows high-level server and agent information.

#### **Prerequisites**

- Register and add the server to be monitored to the Perspective Resources view.
- Authenticate the server.

#### **Task**

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Monitor**.

---

**Note:** You can also view the server status through the status badges on the server icons in the Perspective Resources, Heat Chart, Resource Explorer, and topology views.

---

### **Configuring Data Assurance Server Parameters**

Improve Data Assurance (DA) server performance by editing server system configuration.

#### **Prerequisites**

- Add the server to be monitored to the Perspective Resources view.
- Authenticate the server.

#### **Task**

1. In the Perspective Resources, select a DA server.
2. Select **Resource > Administration Console**.
3. Select **Data Assurance Server**.
4. Select a DA server, then either:
  - Select **Resource > System Configuration** , or,
  - Click the button that appears when you select a DA server, then click **System Configuration**.
5. In the Run Value column, modify the current values of the server parameters.
6. (Optional) Click **Restore to Default** to undo modifications that have not been applied.
7. Click **Apply**.

See the *Replication Server Data Assurance Option Users Guide > Performance and Tuning*.

### **Setting Logging and Audit Levels for Data Assurance Server**

Set the logging and audit trace levels for Data Assurance server.

1. In the Perspective Resources view, select a DA server.
2. Select **Resource > Administration Console**.
3. On the Browse tab, select **Data Assurance Servers**, then select a DA server.
4. Click the button that appears when you select a DA server, then select **Logging Configuration...**
5. Select the audit trace and logging levels.
6. Click **Apply**, then **OK**.



# Troubleshoot SAP Control Center for Data Assurance

Troubleshoot problems that occur in SAP Control Center for Data Assurance.

## Comparison Fails to Detect Differences In LOB Column

Problem: Job comparison results are not recording inconsistencies in database hash column comparisons.

### *Solution 1: Increase LOB Fetch Size*

The inconsistency might exist in a large object (LOB) column, such as `image`. By default, DA server compares only the first 1024 bytes of LOB columns, so some sections of LOB values are not compared.

To solve this problem, increase the **lob\_fetch\_size** value.

### *Solution 2: Increase LOB Fetch Size*

The source and target column values might produce the same MD5/SHA/CRC32 hash value.

To solve this problem, use the **literal** option to recompare the rows.

### **See also**

- *Configuring Data Assurance Server Parameters* on page 156

## External Sort Option Configuration

Problem: You have configured DA agent to perform external sort, but the database is still performing the sort operation.

The enable sort option is not activated because the number of rows in the table is less than the **external\_sort\_activate\_size** value, which by default is 10 million.

Solution: Decrease the **external\_sort\_activate\_size** to a value less than the number of rows in the source and target tables.

### **See also**

- *Configuring Data Assurance Server Parameters* on page 156

## DA Server Out of Memory Errors

---

Problem: DA server runs out of memory space and exhibits performance issues.

### *Solution 1: Decrease Comparer Max Concurrent Threads*

During a comparison, DA server receives row data from DA agents at different rates, so at any given time, the server may be buffering tens or hundreds of rows for each source or target. If individual rows are large (user-database-table-dependent) and the number of comparisons is sufficiently high (configured by the user), this buffering might cause DA server to run out of memory.

To solve this problem, set **comparer\_max\_concurrent\_threads** to a lower value.

### *Solution 2: Decrease LOB Fetch Size*

The configuration parameter **lob\_fetch\_size** may be set to a high value.

To solve this problem, set **lob\_fetch\_size** to a lower value.

### *Solution 3: Decrease External Sort Max Size*

The external sort option uses a large amount of memory. By default, the external sort keeps thousands of rows in memory. While this is not usually a problem, it depends on the size of each row and the simultaneous activity occurring within the same Java Virtual Machine (JVM). For instance, if there are five concurrent comparisons using the DA agent, the memory requirement increases fivefold. Or if the “localagent” is being used, the source and target agents and the compare function are sharing the same JVM memory allocation.

To solve this problem, decrease the number of rows the DA agent stores in the memory by changing the **external\_sort\_max\_size** configuration parameter value.

### *Solution 4: Increase the Memory Available to DA Server*

Global solution: You can address all of the possible causes for out of memory issues described above by configuring DA server to start with more memory. By default, the JVM where the DA server runs uses 512 MB. Increase the value (dependent on the platform and the amount of system memory available) by editing the DA server’s **RUN\_<instance>.bat** file.

### **See also**

- *Configuring Data Assurance Server Parameters* on page 156

## Problems with Basic SAP Control Center Functionality

---

Troubleshoot problems that involve basic features like starting and stopping, authentication, alerts, and scheduling.

## **SAP Control Center Fails to Start**

Problem: The SAP 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 SAP 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 SAP 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 87

## **Cannot Log In**

Problem: Cannot log in to SAP Control Center Web console.

Solution: Make sure that SAP Control Center has been configured:

- To allow logins through the operating system
- To grant appropriate roles to your login account

Ask the SAP Control Center administrator to help you check.

### **See also**

- *User Authorization* on page 90
- *Setting Up Security* on page 69

## **Browser Refresh (F5) Causes Logout**

Problem: Pressing the **F5** key to refresh your browser logs you out of SAP Control Center.

Solution: Do not use **F5** when you are logged in to SAP Control Center. Browser refresh does not refresh data inside SAP Control Center, but refreshes the loaded application or pages in the browser—in this case, the Adobe Flash on which SAP Control Center is built. Consequently,

pressing **F5** logs you out of any servers you are currently logged in to, including SAP Control Center.

### **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 SAP 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 142
- *Graphing Performance Counters: the Statistics Chart* on page 126

### **Resetting the Online Help**

Problem: SAP 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 SAP Control Center.
2. Remove this directory:

```
<SCC-installation-directory>\SCC-3_3\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_3\services
\EmbeddedWebContainer\container\Jetty-6.1.22\contexts
_help.xml
<SCC-installation-directory>\SCC-3_3\services
\SybaseControlCenter\help\com.sybase.infocenter.scc.zip
<SCC-installation-directory>\SCC-3_3\services
\SybaseControlCenter\help\help.war
<SCC-installation-directory>\SCC-3_3\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 SAP 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 132

## **Memory Warnings at Startup**

**Problem:** When SAP 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 61

## **SCC Out of Memory Errors**

**Problem:** SAP Control Center generates `OutOfMemory` errors.

**Solution:**

- If the `OutOfMemory` error says that SAP Control Center is out of heap space, increase the maximum memory setting (*SCC\_MEM\_MAX* or `jvmopt=-Xmx`).
- If the `OutOfMemory` error says that SAP 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 SAP Control Center runs as a service in Windows:  
`C:/windows/system32`

## Troubleshoot SAP Control Center for Data Assurance

- When SAP Control Center runs as a service in UNIX:  
    <SCC-install-directory>/SCC-3\_3/bin  
Send the heap dump files to Technical Support for analysis.

### **See also**

- *Configuring Memory Usage* on page 61

# Glossary: SAP Control Center for Data Assurance

Definitions of SAP Control Center terms related to Replication Server Data Assurance (DA) Option.

**availability** – indicates whether a resource is accessible and responsive.

**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 SAP 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 profile** – information required to establish a database connection.

**database** – a set of related data tables and other objects that are organized and presented to serve a specific purpose.

**Data Assurance job** – a row comparison or a schema comparison job that defines how a compareset is compared and when.

**Data Assurance system database (DASD)** – the DA server database that stores system and configuration settings.

**Data Transfer Stream (DTS)** – an application protocol used by DA agent during a comparison to stream data.

**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.

**heat chart** – a graphical view of resource availability and selected performance and status metrics for all the registered resources in the current perspective.

**inconsistent row** – a table row that is present both in primary and replicate databases, but has different values for one or more of the columns being compared.

**Java Database Connectivity (JDBC)** – an application program interface (API) that allows Java applications to access multiple database management systems using Structured Query Language (SQL).

**jConnect** – the SAP high-performance JDBC driver.

**job** – a task performed by the scheduler in SAP 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.

**managed resource** – see resource.

**missing row** – a table row that is present in the primary, but not in the replicate database.

**orphaned row** – a table row that is present in the replicate, but not in the primary database.

**perspective** – a named tab in SAP 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.

**primary key** – a set of table columns that uniquely identifies each row.

**product module** – a plug-in component of SAP Control Center that manages and monitors a particular Sybase product. SCC product modules are available for SAP ASE, Data Assurance (a Replication Server option), replication (Replication Server, Replication Agent, and Mirror Replication Agent), SAP Sybase Event Stream Processor, and SAP Sybase IQ.

**replication** – a process by which the changes to the data in one database—including creation, updating, and deletion of records—are also applied to the corresponding records in another database.

**repository** – a database in SAP 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 SAP Control Center. Resources SCC can manage include SAP ASE, Data Assurance Server, Replication Server, Replication Agent, Mirror Replication Agent, SAP Sybase Event Stream Processor, SAP Sybase IQ, and certain subcomponents.

**Replication Server Data Assurance (DA) Option** – the SAP server program that compares row data and schema between two or more SAP® Adaptive Server® Enterprise (SAP® ASE) databases and reports discrepancies. In SAP Control Center, the product module that monitors and manages the Replication Server DA Option is called SCC for DA.

**Replication Server system database (RSSD)** – the SAP ASE database containing SAP Replication Server system tables. You can choose whether to store SAP Replication Server system tables on the RSSD or the SAP SQL Anywhere ERSSD.

**Remote Method Invocation (RMI)** – a remote procedure call used for communication between DA server and DA agents.

**SCC agent** – a remote command and control agent for SAP Control Center that runs on a managed server. The SCC agent is installed automatically as part of the Sybase server.

**SCC-enabled login account** – a user account that has been granted privileges in SAP Control Center by mapping appropriate SAP 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 SAP Control Center or created in the operating system or the LDAP directory service to which SAP Control Center authentication is delegated. You must use an SCC-enabled account to log in to SAP Control Center.

**schedule** – the definition of a task (such as the collection of a set of statistics) and the time interval at which SAP Control Center executes the task.

**schema** – the structure of the database.

**Tabular Data Stream (TDS)** – an application protocol by which Open Clients and SAP Open Servers exchange information.

**topology** – a graphical representation of how the servers in an environment are connected to each other. It is a network diagram that provides a visual map of the availability of the environment.

**view (SCC)** – a window in an SAP 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 28, 63
- XX:MaxPermSize permanent memory option 28, 63

## A

- accessibility 11
- Administration Console
  - column filtering 6
  - display tools and options 4
  - displaying only selected resources 127, 128
  - message rows in result sets 128
  - proxy rows 128
  - using 127
- Adobe Flex 11
- agent connection
  - creating 104
  - deleting 151
  - editing 151
  - modifying 151
- alerts
  - effects of repository purging on history 142
- ALL logging level 145
- application menu 2
- audit trace levels
  - setting up 157
- authenticating
  - SCC with a managed resource 17, 100
- authentication
  - about 31, 70
  - configuring for LDAP 34, 74
  - configuring for UNIX 33, 72
  - configuring for Windows 32, 71
- authorization 49, 90
- availability 165

## B

- background, running SCC or SCC agent in 22, 57
- backups
  - about 138
  - changing the schedule 140
  - forcing 140
  - restoring from 141
  - scheduling 139

- suspending and resuming 140
- badges, status 3

## C

- client log, viewing 144
- collections 165
- column comparison problem, database hash 159
- column filtering in SCC 6
- columns
  - sorting by 4
- compare sets
  - creating 109
- compareset
  - deleting 111
  - displaying 111
  - editing 110
  - modifying 110
  - viewing 111
- comparesets 109
- comparison
  - row 112
  - schema 119
- configuration
  - optional 107
- configuring
  - Data Assurance parameters 156
- connections, DA 165
- console
  - about 147
  - commands 148
- conventions, style and syntax 9
- creating
  - a job based on RSSD 118
  - agent connection 104
  - compare sets 109
  - Data Assurance job 112
  - Data Assurance server database connection 105
  - schema comparison job 119
- csi\_config.xml file 34, 74

## D

- DASD 165

## Index

- Data Assurance 166
    - deleting database connection 154
    - key performance indicators 104
  - Data Assurance agent
    - local agent 150
    - remote agent 150
    - standalone agent 150
  - Data Assurance job
    - scheduling 117
  - Data Assurance jobs 165
  - Data Assurance server
    - configuring for monitoring 98
    - creating database connection 105
    - editing database connection 153
    - log file 144
  - Data Assurance system database 165
  - data collection jobs
    - adding 101
    - adding schedules 131
    - creating 101
    - deleting 130
    - displaying history 133
    - executing 130
    - not saving data 101
    - removing schedules 132
    - resuming 130
    - stopping 130
    - suspending 130
    - viewing schedules 132
  - data collection schedules
    - adding 101
    - modifying 132
  - data collections
    - troubleshooting timeouts 163
  - data partition boundaries
    - displaying 111
    - viewing 111
  - Data Transfer Stream in Data Assurance 165
  - database hash column comparison problem 159
  - databases, DA 165
  - DEBUG logging level 145
  - defined 165–167
  - deleting
    - agent connection 151
    - comparison in a row or schema comparison job 122
    - Data Assurance database connection 154
    - Data Assurance job 122
  - display options in SCC 4
  - displaying
    - agent properties, Data Assurance 152
    - compareset 111
    - data partition boundaries 111
    - database connection profiles 154
    - job list, Data Assurance 122
    - topology, Data Assurance 155
  - drivers
    - ODBC, registering 14, 54
  - DTS in Data Assurance 165
- ## E
- editing
    - agent connection 151
    - compareset 110
    - Data Assurance job 117
    - database connection in Data Assurance server 153
    - schema compare 121
    - schema comparison 121
    - system properties, Data Assurance 156
  - environment variables
    - SCC\_MEM\_MAX 26, 28, 29, 61, 63, 64
    - SCC\_MEM\_PERM 26, 28, 29, 61, 63, 64
  - ERROR logging level 145
  - errors
    - OutOfMemory 163
    - REJECT\_DUPLICATE\_RESOURCE\_AND\_COLLECTION policy 163
    - timeouts for data collections 163
  - evaluation
    - quick start instructions 13
  - events 165
  - executing
    - row comparison 121
    - schema comparison 121
  - expiration dates for login accounts 95
  - external sort problem 159
- ## F
- F11 (browser full screen mode toggle) 6
  - F5 (browser refresh)
    - logging out of SAP Control Center 161
  - FATAL logging level 145
  - features, new
    - SAP Control Center for Data Assurance 1
  - Flash Player 15



font size, changing 6  
 foreground, running SCC or SCC agent in 22, 57  
 full backups 139  
 full screen mode 6

## G

getting started after installing 15  
 glossaries  
   SCC for Data Assurance terms 165  
 graphing statistics 126  
 grid format, using 4  
 groups 52, 96  
   adding login accounts 51, 93  
   assigning monitoring and administration roles  
     50, 90  
   creating 51, 91  
   in LDAP, mapping to SCC roles 44, 84  
   in OS, mapping to SCC roles 44, 84  
   remove login 93  
   removing 92  
   removing roles 91  
   SCC Administrator 44, 84  
   sybase 44, 84

## H

heat chart 165  
   customizing columns 17, 125  
   display tools and options 4  
   displaying 17, 125  
   filtering resources displayed 17, 125  
   icons 3  
   launch icon 2  
 help command (console) 148  
 historical performance monitoring 126

## I

icons  
   for server status 3  
   in SCC toolbar 2  
   minimize/maximize sections of a view 6  
 importing  
   connection 107  
   interface file 107  
 inconsistent row, DA 165  
 incremental backups 139  
 info command (console) 148

INFO logging level 145  
 interfaces files, importing resources from 99

## J

Java system properties  
   displaying information about 148  
 jConnect 165  
 JDBC 165  
 job history  
   deleting 123  
   viewing report 123  
 job history results 123  
 jobs 165  
   creating Data Assurance 112  
   Data Assurance 112  
   deleting history results 123  
   editing Data Assurance 117  
   modifying collection intervals 132  
   modifying Data Assurance 117  
   resuming 132  
   suspending 132  
 jvmopt memory options for Windows services 26,  
   28, 61, 63

## K

key performance indicators 165  
   Data Assurance 104  
   getting values from heat chart icons 17, 125  
 keyboard shortcuts 7  
 keyboard shortcuts for Adobe Flex 11  
 KPIs 165

## L

layout for SCC views 138  
 LDAP  
   configuration properties 36, 75  
   configuring authentication 34, 74  
   configuring to authenticate SCC logins 31, 70  
 local agent 150  
 log4j.properties file 146  
 logging in to SAP Control Center 29, 68  
   troubleshooting 161  
 logging in to SAP Control Center - first user 15  
 logging levels 145  
 logging out of SAP Control Center 69  
   unintentionally, using F5 browser refresh 161

## Index

- login accounts
  - assigning monitoring and administration roles 50, 90
  - authenticating 17, 100
  - creating automatically (UNIX) 33, 72
  - creating automatically (Windows) 32, 71
  - default 94
  - expiration date, imposing 95
  - granting privileges with roles and groups 44, 84
  - modifying 95
  - native SCC, adding 94
  - predefined 52, 96
  - removing 95
  - removing roles 91
  - suspending 95

- login accounts, default
  - about 15

- login modules 31, 70

- login session timeout 69
  - setting 49, 89

- logs

- agent log, viewing 144
- alert services log, about 143
- changing the logging level 145
- client log, about 143
- client log, viewing 144
- component logs, about 143
- configuring 146
- Data Assurance logs, viewing 144
- repository log, about 143
- repository log, viewing 144
- SCC agent log, about 143
- script execution log, about 143
- server logs, about 143
- server logs, viewing 144

## M

- managed resources 133, 166

- managed servers

- See managed resources

- memory

- configuring 26, 61
- displaying information about 148
- warnings at startup 163

- memory leak 163

- memory, insufficient 161

- menus, application and view 2

- message levels 145

- message rows

- using 128

- minimize/maximize icon 6

- missing rows, DA 166

- modifying

- agent connection 151
- compareset 110
- Data Assurance job 117
- schema compare 121
- schema comparison 121

- monitor

- Data Assurance agent 18, 156
- Data Assurance server 18, 156

- monitoring

- Data Assurance 155
- performance 126

## N

- new features

- SAP Control Center for Data Assurance 1

## O

- ODBC drivers

- registering 14, 54

- online help

- resetting 162

- operating system

- configuring to authenticate SCC logins 31, 70

- orphaned row, DA 166

- out of memory error, DA server 160

- OutOfMemory errors, SCC 163

## P

- parameters

- configuring Data Assurance 156

- passencrypt utility 46, 86

- passwords

- encrypting 46, 86

- for repository database dba account, changing 64

- for SCC default login account 15

- performance monitoring 126

- Perspective Heat Chart view 17, 125

- Perspective Resources view

- about 133, 136

- display tools and options 4

- icons 3
  - show/hide icon 2
- perspectives 166
  - about 136
  - adding resources 134
  - creating 136
  - removing 136
  - removing a resource 134
  - renaming 136
- pluggable authentication modules for UNIX
  - authentication 33, 72
- port conflicts 161
- ports
  - changing 64
  - configuring 47, 87
  - default 64
  - displaying information about 148
- postinstallation tasks 15
- primary key, DA 166
- product modules 166
  - displaying versions 8
- production environment, setting up SCC in 19
- properties
  - for resources, changing 135

## Q

- quick start instructions 13

## R

- Red Hat Linux authentication 34, 73
- registration
  - about 133
- REJECT\_DUPLICATE\_RESOURCE\_AND\_COLLECTION policy errors 163
- Remote Method Invocation (DA) 166
- replication 166
- Replication Server Data Assurance Option 166
  - data collection 103
  - database connections 153
- Replication Server system database 166
- repository 138, 166
  - backing up 140
  - changing backup schedule 140
  - changing database dba password 64
  - configuring purging 142
  - restoring from backup 141
  - scheduling backups 139

- resource explorer
  - launch icon 2
- Resource Explorer
  - about 133
  - display tools and options 4
  - searching in 135
- resources 166
  - about 133
  - adding to a perspective 134
  - authenticating 17, 100
  - browsing and managing 127
  - changing connection properties 135
  - changing name 135
  - displaying availability 17, 125
  - filtering by column in Admin Console 4
  - importing in batch 99
  - modifying data collection schedules 132
  - removing from a perspective 134
  - searching and filtering in Admin Console 128
  - searching for 135
  - selecting for display in Admin Console 128
  - unregistering 133
- resources, Data Assurance
  - registering with SAP Control Center 16, 98
- restarts
  - configuring in UNIX 22, 57
  - configuring in Windows 19, 55
- RMI (DA) 166
- role-mapping.xml file 44, 84
- roles
  - assigning to users and groups 50, 90
  - mapping SCC roles to LDAP or OS groups 44, 84
  - predefined 52, 96
  - product level 49, 90
  - removing 91
  - system level 49, 90
- row comparison
  - executing 121
  - running 121
- RSSD 166
- RSSD user name, using to authenticate 17, 100
- running
  - row comparison 121
  - schema comparison 121

## S

- SAP Control Center
  - accessibility 11

## Index

- connecting a browser to 15
- console commands 148
- display tools and options 4
- displaying component versions 8
- failure to start 161
- keyboard shortcuts 7
- log files 144
- logging in 29, 68
- logging out 69
- logging out unintentionally with F5 161
- starting 14, 54
- starting in UNIX 22, 57
- starting in UNIX as a service 22, 57
- starting in Windows 19, 55
- starting in Windows as a service 19, 55
- stopping in UNIX 22, 57
- stopping in Windows 19, 55
- SAP Control Center for Data Assurance
  - about 1
  - new features 1
- Save data collected from this job checkbox 101
- SCC Administrator group 44, 84
- SCC agent 166
  - starting in UNIX 22, 57
  - starting in UNIX as a service 22, 57
  - starting in Windows 19, 55
  - starting in Windows as a service 19, 55
  - stopping in UNIX 22, 57
  - stopping in Windows 19, 55
- scc command 64
  - using to launch SAP Control Center 14, 54
- SCC\_MEM\_MAX 26, 28, 29, 61, 63, 64, 163
- SCC\_MEM\_PERM 26, 28, 29, 61, 63, 64
- SCC-enabled login account 167
- scc.bat 14, 19, 54, 55
- scc.sh 22, 57
- sccadmin account
  - about 15
- sccAdminRole 52, 96
- sccd shell script 22, 57
- sccUserRole 52, 96
- scheduler
  - resuming 132
  - suspending 132
- schedules 129, 167
  - adding to a job 131
  - creating for a data collection job 101
  - removing from a job 132
  - viewing 132
- scheduling
  - Data Assurance job 117
- schema compare
  - editing 121
  - modifying 121
  - updating 121
- schema comparison
  - creating 119
  - editing 121
  - executing 121
  - modifying 121
  - running 121
  - setting up 119
  - updating 121
- schema, DA 167
- screens
  - maximizing 6
  - maximizing and minimizing sections of a view 6
- security 31, 70
  - configuring 30, 69
- security providers
  - configuring 31, 70
- server log, viewing for Data Assurance 144
- server logs, viewing 144
- servers
  - authenticating 17, 100
  - displaying availability 17, 125
  - importing in batch 99
  - modifying data collection schedules 132
  - searching for 135
  - unregistering 133
- servers, Data Assurance
  - registering with SAP Control Center 16, 98
- services
  - enabling and disabling 64
  - listing 148
- services, UNIX
  - configuring SCC memory options for 29, 64
  - running SCC or SCC agent as 22, 57
- services, Windows
  - configuring SAP Control Center memory options for 28, 63
  - running SCC or SCC agent as 19, 55
- setting up
  - schema comparison job 119
- shutdown command (console) 149
- sorting by column 4
- sql.ini files, importing resources from 99

- standalone agent 150
- start up
  - automatic, configuring in UNIX 22, 57
  - automatic, configuring in Windows 19, 55
- starting SAP Control Center 14, 54
- states
  - Data Assurance 104
- statistics
  - about 103
  - availability 103
  - performance 103
- statistics chart
  - displaying data for a longer period 162
  - effects of repository purging on 142
  - graphing performance counters 126
  - troubleshooting 162
- status command (console) 150
- status icons and badges for resources 3
- SUSE Linux authentication 34, 73
- sybase group 44, 84
- system properties
  - displaying information about 148
- system-wide features
  - configuring 30, 69

## T

- Tabular Data Stream 167
- TDS 167
- terms
  - SCC for Data Assurance 165
- testing
  - agent connection 152, 154
- text conventions 9
- timeout
  - errors on data collections 163
  - setting for login sessions 49, 89
- toolbar icons 2
- topology, DA 167
- topology, Data Assurance
  - displaying 155
  - viewing 155
- troubleshoot
  - database hash column comparison problem 159
  - external sort problem 159
  - out of memory error 160
- troubleshooting
  - Data Assurance 159

## U

- UNIX
  - configuring authentication 33, 72
  - running SCC or SCC agent in the background 22, 57
  - running SCC or SCC agent in the foreground 22, 57
  - starting, stopping SCC or SCC agent 22, 57
- updating
  - schema compare 121
  - schema comparison 121
- user accounts
  - default 94
  - native SCC, adding 94
  - native SCC, not using 31, 70
- user information
  - modifying 95
- user interface, about 2

## V

- versions of SCC components
  - displaying 8
- View menu 6
- viewing
  - agent properties, Data Assurance 152
  - compareset 111
  - Data Assurance job report 123
  - Data Assurance job status 123
  - Data Assurance jobs 122
  - data partition boundaries 111
  - job history report 123
  - topology, Data Assurance 155
- views
  - maximizing and minimizing sections 6
- views, SCC 167
  - about 137
  - arranging in perspective 138
  - bringing to front of perspective 137
  - closing 137
  - icons for managing 2
  - maximizing 137
  - menus 2
  - minimizing 137
  - opening 137
  - restoring 137

Index

## **W**

WARN logging level 145

## **Windows**

configuring authentication 32, 71

starting, stopping SCC or SCC agent 19, 55