SYBASE®

Sybase Control Center

Sybase Control Center 3.1

DOCUMENT ID: DC01264-01-0310-01
LAST REVISED: February 2010

Sybase, Inc., One Sybase Drive, Dublin, CA 94568.

Contents

Get Started

Begin using Sybase® Control Center.

About Sybase® Control Center

Sybase Control Center is a server application that uses a Web-browser-based client to deliver an integrated solution for monitoring and managing Sybase products.

Sybase Control Center provides a single comprehensive Web administration console for real-time performance, status, and availability monitoring of large-scale Sybase enterprise servers. Sybase Control Center combines a modular architecture, a rich client administrative console, agents, common services, and tools for managing and controlling Sybase products. It includes historical monitoring, threshold-based alerts and notifications, alert-based script execution, and intelligent tools for identifying performance and usage trends.

A Sybase Control Center server can support:

- Up to 50 monitored resources (servers)
- Up to 10 users logged in simultaneously

Toolbar Icons

Describes the icons in the Sybase Control Center toolbar.

Table 1. Toolbar icons

Icon	Name	Description
	**Show/Hide resource browser**	Displays or minimizes the Perspective Resources view.
	**Launch resource explorer**	Opens the resource explorer.
	**Launch heat chart**	Opens the perspective heat chart.
	**Close all open views**	Closes all open and minimized views.
	**Minimize all views**	Minimizes all open views.
	**Restore all minimized views**	Returns all minimized views to their original size.

Icon	Name	Description
	**Cascade all open views**	Arranges open views to overlap each other.
	**Tile all open views vertically**	Arranges open views in a vertical manner.
	**Tile all open views horizontally**	Arranges open views in a horizontal manner.

See also

- *Status Icons* on page 2
- *Common Display Options* on page 3
- *Accessibility Features* on page 5
- *Sybase Control Center Accessibility Information* on page 5

Status Icons

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

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.

Table 2. Resource status icons: Perspective Resources view and heat chart

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

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

Table 3. KPI status icons: heat chart

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

See also

- *Toolbar Icons* on page 1
- *Common Display Options* on page 3
- *Accessibility Features* on page 5
- *Sybase Control Center Accessibility Information* on page 5

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

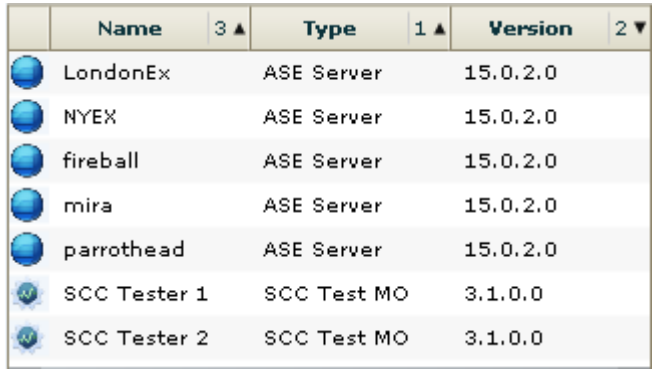
Table 4. Column sorting options

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) changes to point 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.

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

The figure below shows a table of servers sorted first by resource type; within type by software version; and within version by server name. The Type and Name columns sort in ascending order and the Version column sorts in descending order. (In this case, the direction of the Version column sort has no effect because all the versions within each resource type are the same.)

Figure 1: Resources sorted by type, version, and name



Maximize a section of a view. Some areas within views have a square minimize/maximize panel in the upper right corner. Click the panel to expand that area to fill the entire view. Click the panel again to reduce 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.

See also

- *Toolbar Icons* on page 1
- *Status Icons* on page 2
- *Accessibility Features* on page 5
- *Sybase Control Center Accessibility Information* on page 5

Accessibility Features

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

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

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

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

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

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

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

See also

- *Toolbar Icons* on page 1
- *Status Icons* on page 2
- *Common Display Options* on page 3
- *Sybase Control Center Accessibility Information* on page 5

Sybase Control Center Accessibility Information

Sybase Control Center uses the Adobe Flex application.

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

Note: To use Sybase Control Center with JAWS for Windows screen reading software effectively, download and install the appropriate Adobe scripts. See *www.adobe.com*.

See also

- *Toolbar Icons* on page 1
- *Status Icons* on page 2
- *Common Display Options* on page 3
- *Accessibility Features* on page 5

Setting Up Security

Configure login authentication, specify an e-mail server, and map roles.

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

1. *Security*

   The Sybase Control Center security model delegates user authentication to the operating system or to your LDAP server.
2. *Configuring Authentication for Windows*

   Authentication through the Windows operating system is enabled by default, but it requires some configuration. First, set Sybase Control Center to create an account when a Windows user logs in to Sybase Control Center.
3. *Configuring a Pluggable Authentication Module (PAM) for UNIX*

   Set up Sybase Control Center to support username and password login using accounts on the UNIX operating system. Optionally, have Sybase Control Center create an account when a UNIX user first logs in to Sybase Control Center.
4. *Configuring an LDAP Authentication Module*

   Configure an LDAP authentication module for Sybase Control Center by editing the security properties file to point to the correct LDAP server.
5. *Mapping Sybase Control Center Roles to LDAP or OS Groups*

   To grant Sybase Control Center privileges to users who are authenticated through LDAP or the operating system, associate roles used in Sybase Control Center with groups in LDAP or the operating system.
6. *Configuring the E-mail Server*

   Specify the e-mail server for Sybase Control Center to use to send e-mail alert notifications.
7. *Configuring Sybase Control Center*

   For configuration instructions, see the Configure section of the help for your Sybase Control Center product module.

Security

The Sybase Control Center security model delegates user authentication to the operating system or to your LDAP server.

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

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

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

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

Sybase Control Center provides a set of predefined login modules for authentication. All login modules are defined in the `<install_location>/SCC-3_1/conf/csi.properties` file. The syntax is defined by the Sybase Common Security Infrastructure (CSI) framework. You can configure the different login modules to customize security strength. The login modules are:

- Simple Login – defines a user name, password, and a list of roles. The default user name is “sccadmin” with a blank password and a native role of “sccAdminRole”. You can create additional accounts by adding simple login modules to `csi.properties`. However, Sybase does not recommend the use of simple login modules for authentication in production environments.

  Note: Add a password for the sccadmin account as soon as possible after you install Sybase Control Center. See the *Sybase Control Center Installation Guide* for instructions.
- NT Proxy Login – delegates authentication to the underlying Windows operating system. When you log in to Sybase Control Center through an NT Proxy Login module, enter your user name in the format *username@nt-domain-name*. For example, user@sybase. Windows authentication is enabled by default, but it requires some configuration.
- UNIX Proxy Login – delegates authentication to the underlying UNIX or Linux operating system using Pluggable Authentication Modules (PAM). When you log in to Sybase

Control Center through a UNIX PAM, enter only your user name. UNIX authentication is enabled by default, but it requires some configuration.

- LDAP Login – delegates authentication to an LDAP server you specify. When you log in to Sybase Control Center through an LDAP server, enter only your user name. LDAP authentication is not enabled by default; you must configure the login module.

See also

- *Configuring Authentication for Windows* on page 8

Configuring Authentication for Windows

Authentication through the Windows operating system is enabled by default, but it requires some configuration. First, set Sybase Control Center to create an account when a Windows user logs in to Sybase Control Center.

This task is optional. However, if you choose not to create Sybase Control Center accounts automatically as described here, you must enter them manually. Sybase Control Center needs the accounts for purposes of setting authorization (user privileges).

1. Log in to Sybase Control Center using an account with administrative privileges (sccAdminRole).
2. Select **Application** > **Administration** > **Security.**
3. Check the box labeled **Automatically add SCC login records for authenticated logins**.
4. Click **OK** to close the Security dialog.

Next

There are two next steps:

- If you opted not to automatically create Sybase Control Center login accounts, follow the steps in Adding a Login to the System to enter each account into Sybase Control Center manually.
- Whether you add accounts automatically or manually, you must also grant privileges to the login accounts. You can grant privileges by assigning Sybase Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping Sybase Control Center roles to the groups. The group approach is generally more efficient.

See also

- *Security* on page 7
- *Configuring a Pluggable Authentication Module (PAM) for UNIX* on page 9

Configuring a Pluggable Authentication Module (PAM) for UNIX

Set up Sybase Control Center to support username and password login using accounts on the UNIX operating system. Optionally, have Sybase Control Center create an account when a UNIX user first logs in to Sybase Control Center.

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 Sybase Control Center) to the `/etc/pam.conf` file on your Solaris platform.
Linux	Copy the `<SCC-install-dir>/utility/linux/sybase-ua` file (provided with Sybase Control Center) to the `/etc/pam.d` directory on your Linux platform. **Note:** The `sybase-ua` file provided with Sybase Control Center is not compatible with the most recent SUSE Linux versions. For SUSE 11 and later, see the example at the end of this topic.
HP-UX	Append the contents of the `<SCC-install-dir>/utility/hpux/pam.conf` file (provided with Sybase Control Center) to the `/etc/pam.conf` file on your HP-UX platform.
AIX	Create or edit the `/etc/pam.conf` file and include the contents of `<SCC-install-dir>/utility/aix/pam.conf` (provided with Sybase Control Center).

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

2. (Skip if you configured a PAM before starting Sybase Control Center) Reboot Sybase Control Center.
3. (Optional) If you want Sybase Control Center to create an account when a UNIX user logs in to Sybase Control Center, execute these steps. If you choose not to create Sybase Control Center accounts automatically, you must enter them manually. Sybase Control Center needs the accounts for purposes of setting authorization (user privileges).
   a) Log in to Sybase Control Center using an account with administrative privileges (sccAdminRole).
   b) Select **Application** > **Administration** > **Security.**
   c) Check the box labeled **Automatically add SCC login records for authenticated logins**.
   d) Click **OK** to close the Security dialog.

Example: PAM for SUSE Linux 11 and later

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

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

Next

There are two next steps:

- If you opted not to automatically create Sybase Control Center login accounts, follow the steps in Adding a Login to the System to enter each account into Sybase Control Center manually.
- Whether you add accounts automatically or manually, you must also grant privileges to the login accounts. You can grant privileges by assigning Sybase Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping Sybase Control Center roles to the groups. The group approach is generally more efficient.

See also

- *Configuring Authentication for Windows* on page 8
- *Configuring an LDAP Authentication Module* on page 10

Configuring an LDAP Authentication Module

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

1. Open the `<SCC-install-dir>\conf\csi.properties` file.
2. Uncomment the LDAP module in the properties file by removing the # symbol at the beginning of each line (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 for values that work for ActiveDirectory. Configuration properties you can use in the LDAP module are described in a subtopic.

   Each line of the LDAP server module of the properties file must begin with "CSI.loginModule." followed by a module number. (The module number in this sample is 7.) The module number you assign must be unique in the properties file, and you must use the same module number in every line of the module.

   ```
   CSI.loginModule.
   7.options.AuthenticationSearchBase=ou=users,dc=example,dc=com
   CSI.loginModule.7.options.BindDN=cn=Directory Manager
   CSI.loginModule.7.options.BindPassword=secret
   ```

```
CSI.loginModule.7.options.DefaultSearchBase=dc=example,dc=com
CSI.loginModule.7.options.ProviderURL=ldap://localhost:10389
CSI.loginModule.
7.options.RoleSearchBase=ou=groups,dc=example,dc=com
CSI.loginModule.7.options.ServerType=openldap
CSI.loginModule.7.options.moduleName=LDAP Login Module
CSI.loginModule.7.controlFlag=sufficient
CSI.loginModule.
7.provider=com.sybase.ua.services.security.ldap.LDAPLoginModule
```

Note: Change the values of bolded lines only.

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:

```
keytool -import -keystore <sybase-dir>/shared/JRE-6_0_6/bin/
keytool/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

There are two additional steps:

- Set up roles and passwords for LDAP
- Map Sybase Control Center role to LDAP groups

See also

- *Configuring a Pluggable Authentication Module (PAM) for UNIX* on page 9
- *Mapping Sybase Control Center Roles to LDAP or OS Groups* on page 19

Setting Up Roles and Passwords

Set the initial user roles and passwords required for Sybase Control Center to authenticate through an LDAP server.

Prerequisites

Configure an LDAP authentication module.

1. Open the `<SCC-install-dir>\conf\roles-map.xml` file and add an LDAP login module.

   Insert an LDAP login module similar to this at the end of the security-modules portion of the file, just before `</security-modules>`:

   ```
       <module name="LDAP Login Module">
         <role-mapping modRole="sybase"
   uafRole="uaAnonymous,uaPluginAdmin,sccUserRole" />
         <role-mapping modRole="administrators"
   uafRole="uaAnonymous,sccAdminRole" />
       </module>
   ```

2. Ensure that the roles defined in the LDAP repository match the roles defined in `roles-map.xml`.
3. In the `<SCC-install-dir>\conf\csi.properties` 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.properties`.

Next

Map Sybase Control Center roles to LDAP groups.

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 properties file. Enter the password in clear text (unencrypted) when you execute **passencrypt** and when you use the password to log in.

passencrypt, which is located in the Sybase Control Center `bin` directory, uses the DES encryption algorithm.

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

   Windows: `cd <SCC-install-directory>\bin`
   UNIX: `cd <SCC-install-directory>/bin`

2. Encrypt a password:

   ```
   passencrypt -text <new_password>
   ```

The passencrypt utility encrypts the password you enter and displays the password in encrypted form.

3. Copy the encrypted password.
4. Paste the encrypted password where needed.
5. When you have encrypted all the passwords you need, immediately close the command window—it displays passwords in clear text.

LDAP Configuration Properties

Use these properties in your `csi.properties` file to control your LDAP service.

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

Property	Default Value	Description
DefaultSearchBase	None	Tthe LDAP search base that is used if no other search base is specified for authentication, roles, attribution and self registration: 1. `dc=<domainname>,dc=<tld>` For example, a machine in sybase.com domain would have a search base of dc=sybase,dc=com. 2. `o=<company name>,c=<country code>` For example, this might be o=Sybase,c=us for a machine within the Sybase organization.
SecurityProtocol	None	The protocol to be used when connecting to the LDAP server. To use an encrypted protocol, use "ssl" instead "ldaps" in the url. **Note:** ActiveDirectory requires the SSL protocol when setting the value for the password attribute. This occurs when creating a user or updating the password of an existing user.
AuthenticationMethod	simple	The authentication method to use for all authentication requests into LDAP. Legal values are generally the same as those of the java.naming.security.authentication JNDI property. Choose one of: • simple — For clear-text password authentication. • 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. See the*Java Sun* Web site for more information.

Property	Default Value	Description
AuthenticationFilter	For most LDAP servers: `(&(uid={uid})(objectclass=person))` or For Active Directory email lookups: `(&(userPrincipalName={uid})(objectclass=user))[ActiveDirectory]` For Active Directory Windows username lookups: `(&(sAMAccountName={uid})(objectclass=user))`	The filter to use when looking up the user. When performing a username based lookup, this filter is used to determine the LDAP entry that matches the supplied username. The string "{uid}" in the filter is replaced with the supplied username.
AuthenticationScope	onelevel	The authentication search scope. The supported values for this are: • `onelevel` • `subtree` If you do not specify a value or if you specify an invalid value, the default value is used.
AuthenticationSearchBase	none	The search base used to authenticate users. If this value is not specified, the LDAP DefaultSearchBase is used.

Property	Default Value	Description
BindDN	none	The user DN to bind against when building the initial LDAP connection. 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. However, the LDAP attributer may also use this DN to create the users in the LDAP server. When the self-registration feature is used, this user may also need the requisite permissions to create a user record. This behavior can occur if you do not set useUserCredentialsToBind to `true`. In this case, the LDAP attributer uses this DN to update the user attributes.
BindPassword	none	BindPassword is the password for BindDN, which is used to authenticate any user. BindDN and BindPassword are used to separate the LDAP connection into units. The AuthenticationMethod property determines the bind method used for this initial connection. If you encrypt the password, append .e to the property name. For example: `CSI.loginModule.7.options.BindPassword.e=1-AAAAEgQQOLL+LpXJO8fO9T4SrQYRC9lRT1w5ePfdczQTDsP8iACk9mDAbm3F3p5a1wXWKK8+NdJuknc7w2nw5aGJlyG3xQ==`
RoleSearchBase	none	The search base used to retrieve lists of roles. If this value is not specified, the LDAP DefaultSearchBase is used.

Property	Default Value	Description
RoleFilter	For SunONE/iPlanet: `(&(objectclass=ldapsubentry) (objectclass=nsroledefinition))` For Netscape Directory Server: (`objectclass=groupofnames) (objectclass=groupofuniquenames`)) For ActiveDirectory: `(objectclass=groupofnames) (objectclass=group))`	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 or this property is not initialized, no roles are available.
RoleMemberAttributes	For Netsape Directory Server: member,uniquemember	The role's member attributes defines a comma-delimited list of attributes that roles may have that define a list of DN's of people who are in the role. 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 only has a default value when the Netscape server type is chosen.
RoleNameAttribute	cn	The attribute for retrieved roles that is the common name of the role. If this value is "dn" it is interpreted specially as the entire dn of the role as the role name.
RoleScope	onelevel	The role search scope. The supported values for this are: • `onelevel` • `subtree` If you do not specify a value or if you specify an invalid value, the default value is used.

Property	Default Value	Description
UserRoleMembershipAttributes	For iPlanet/SunONE: nsRoleDN For ActiveDirectory: memberOf For all others: none	The user's role membership attributes property is used to define an attribute that a user has that contains the DN's of all of the roles as user is a member of. These comma-delimited values are then cross-referenced with the roles retrieved in the role search base and search filter to come up with a list of user's roles.
UserFreeformRoleMembershipAttributes	None	The "freeform" 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 user's LDAP record has the following values for the department attribute, { "sales", "consulting" }, then the user will be granted roles whose names are "sales" and "consulting".
Referral	ignore	The behavior when a referral is encountered. The valid values are those dictated by LdapContext, for example, "follow", "ignore", "throw".
DigestMD5Authentication-Format	DN For OpenLDAP: Username	The DIGEST-MD5 bind authentication identity format.
UseUserAccountControlAttribute	For most LDAP servers: false For ActiveDirectory: true	The UserAccountControl attribute to be used for detecting disabled user accounts, account expirations, password expirations and so on. ActiveDirectory also uses this attribute to store the above information.
controlFlag	optional	Indicates whether authentication with this login module is sufficient to allow the user to log in, or whether the user must also be authenticated with another login module. Rarely set to anything other than "sufficient" for any login module. **Note:** controlFlag is a generic login module option rather than an LDAP configuration property.

Mapping Sybase Control Center Roles to LDAP or OS Groups

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

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

By default, Sybase Control Center assumes there is a "sybase" group in the authenticating system and maps the LDAP or OS "sybase" group to Sybase Control Center roles to provide basic privileges. The table lists additional default mappings of LDAP and OS groups to Sybase Control Center roles.

Login module	OS group	Sybase Control Center roles
UNIX Proxy	root	uaAnonymous, uaAgentAdmin, uaOSAdmin
	sybase	uaAnonymous, uaPluginAdmin, sccUserRole
	user	uaAnonymous, uaUser
	guest	uaAnonymous, uaGuest
NT Proxy	Administrators	uaAnonymous, uaAgentAdmin, uaOSAdmin
	sybase	uaAnonymous, uaPluginAdmin, sccUserRole
	Users	uaAnonymous, uaUser
	Guests	uaAnonymous, uaGuest
LDAP	sybase	uaAnonymous, uaPluginAdmin, sccUserRole

There are two ways to accomplish the mapping:

- (Recommended) Add a "sybase" group to the operating system or LDAP server Sybase Control Center is using to authenticate users, and add all users who need to access Sybase Control Center to the "sybase" group.
- Configure Sybase Control Center to use an existing group in LDAP or the operating system by editing the `roles-map.xml` file. This option is described here.

1. If Sybase Control Center is running, shut it down.
2. In a text editor, open:

   `<SCC-install-directory>/conf/roles-map.xml`
3. Locate the appropriate login module (UNIX or NT (for Windows)).

4. Copy the line that maps the “sybase” group and paste it into the module just above the original sybase line.
5. Change “sybase” to the name of the group in your operating system to which Sybase Control Center users belong.

   For example, if the group is SCCusers, the new line should look like this:

   ```
   <role-mapping modRole="SCCusers"
   uafRole="uaAnonymous,uaPluginAdmin,sccUserRole" />
   ```
6. Save the file and exit.
7. Start Sybase Control Center.

See also

- *Configuring an LDAP Authentication Module* on page 10
- *Configuring the E-mail Server* on page 20
- *Assigning a Role to a Login or a Group* on page 30
- *User Authorization* on page 29

Configuring the E-mail Server

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

Prerequisites

Launch Sybase Control Center and log in.

1. From the menu bar, select **Application > Administration.**
2. Select **General Settings**.
3. Enter the name of the e-mail server through which Sybase Control Center will send alert notifications.
4. Change the default e-mail server port only in consultation with your e-mail administrator.
5. (Optional) Enter an e-mail address and click **Send** to dispatch a test message.
   If the test e-mail is received, you have properly configured the server for e-mail alert notifications.
6. Click **Apply**, then click **OK**.

See also

- *Mapping Sybase Control Center Roles to LDAP or OS Groups* on page 19
- *Configuring Sybase Control Center* on page 21
- *Launching Sybase Control Center* on page 21
- *Logging in to Sybase Control Center* on page 28

Configuring Sybase Control Center

For configuration instructions, see the Configure section of the help for your Sybase Control Center product module.
If you have more than one product module installed, follow the configuration instructions for each module.

See also

- *Configuring the E-mail Server* on page 20

Launching Sybase Control Center

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

Prerequisites

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

1. Start Sybase Control Center.
   - Windows – navigate to `<install_location>\sybase\SCC-3_1\bin` and double-click **scc.bat**.
   - UNIX – execute **scc.sh**.

   Messages on the progress of the launch appear in a command window. When Sybase Control Center is running, the command window becomes the Sybase Control Center console; you can issue commands to get status information on Sybase Control Center and its ports, plug-ins, and services.
2. Open a Web browser and enter `https://<hostname>:8283/scc`.

Next

See the Windows and UNIX subtopics for instructions on stopping Sybase Control Center and running it as a service.

See also

- *Sybase Control Center Console* on page 63

Starting and Stopping Sybase Control Center in Windows

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

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

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

  Note: To start or stop Sybase Control Center as a service, you must have selected **Yes** in the installer to install Sybase Control Center as a service.

The installer attempts to start Sybase Control Center as a service and configures the service to restart automatically. Before starting, check the Windows Services list for a Sybase Control Center service.

- Start Sybase Control Center:
  a) (Recommended) Change to the `Sybase` directory immediately above the installation directory and run **SYBASE.bat**.
  b) If you are starting Sybase Control Center for the first time in Windows Vista, access the command prompt as an administrator so that Sybase Control Center can register its ODBC driver.
  c) Enter:
  ```
  %SYBASE%\SCC-3_1\bin\scc.bat
  ```
- Stop Sybase Control Center:
  a) (Recommended) Change to the `Sybase` directory immediately above the installation directory and run **SYBASE.bat**.
  b) Enter:
  ```
  %SYBASE%\SCC-3_1\bin\scc.bat --stop
  ```

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

- Start or stop from the Windows Control Panel; configure automatic start and restart:
  a) Open the Windows Control Panel.
  b) Select **Administrative Tools** > **Services.**
  c) Locate Sybase Control Center 3.1. If the service is running, the status column displays "Started."
  d) To start or stop the service, right-click Sybase Control Center 3.1 and choose **Start** or **Stop**.
  e) To configure automatic starting, double-click the service.
  f) To set the service to automatically start when the system starts, change the **Startup type** to Automatic.
  g) To restart the service in case of failure, choose the **Recovery** tab and change the First, Second, and Subsequent failures to Restart Service.
  h) Click **Apply** to save the modifications and close the dialog.
- Start or stop the Sybase Control Center service from the Windows command line:
  a) To start the service, enter:

```
net start "sybase control center 3.1"

The Sybase Control Center 3.1 service is starting......
The Sybase Control Center 3.1 service was started
successfully.
```

  b) To stop the service, enter:

```
net stop "sybase control center 3.1"

The Sybase Control Center 3.1 service is stopping.....
The Sybase Control Center 3.1 service was stopped
successfully.
```

See also

- *Starting and Stopping Sybase Control Center in UNIX* on page 23
- *scc Command* on page 25

Starting and Stopping Sybase Control Center in UNIX

There are two ways to start Sybase Control Center. You can start it 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.

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

- Use the **scc.sh** script to start Sybase Control Center manually. The command gives you access to the Sybase Control Center console, which you can use to shut down and to

display information about services, ports, system properties, and environment variables. You can also use **scc.sh** to run Sybase Control Center at a nondefault logging level for troubleshooting. When you use **scc.sh**, you cannot take advantage of the automatic start and restart features available to services.

- Use the **agentd** script to configure a Sybase Control Center service that starts automatically.

Here are the steps:

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

     Bourne shell:

     ```
     . SYBASE.sh
     ```

     C shell:

     ```
     source SYBASE.csh
     ```
- **Start Sybase Control Center manually.**
  a) To start Sybase Control Center and drop into the console when the startup sequence is finished, enter:

     ```
     $SYBASE/SCC-3_1/bin/scc.sh
     ```
- **Shut down Sybase Control Center.**
  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:

     ```
     $SYBASE/SCC-3_1/bin/scc.sh --stop
     ```
- **Configure Sybase Control Center 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. In UNIX installations, a shell script, **agentd**, is available in `$SYBASE/SCC-3_1/bin`. Use **agentd** to configure the Sybase Control Center service. (Some UNIX platforms supply tools that make service configuration easier; Linux **chkconfig** is an example.)

  Note: Sybase recommends that if you are not familiar with the process of 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 `agentd` into this directory:

- HPUX: `/sbin/init.d`
- AIX: `/etc/rc.d/init.d`
- All other platforms: `/etc/init.d`

b) Open `agentd` and edit the line that sets the *SYBASE* variable. Set it to the location of your Sybase installation (that is, the parent of `SCC-3_1`, the Sybase Control Center installation directory).

c) On Linux, execute this command to configure the service to run in run levels 2, 3, 4, and 5:

```
/usr/sbin/chkconfig --add agentd
```

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

d) On other UNIX platforms, make two soft links in this directory:

- HPUX: `/sbin/rcX.d`
- AIX: `/etc/rc.d/rcX.d`
- All other platforms: `/etc/rcX.d`

Where X is the run level (for example, 3). Set the links to point to:

- HPUX: `/sbin/init.d/agentd: S90agentd` and `/sbin/init.d/agentd: K10agentd`
- AIX: `/etc/rc.d/init.d/agentd: S90agentd` and `/etc/rc.d/init.d/agentd: K10agentd`
- All other platforms: `/etc/init.d/agentd: S90agentd` and `/etc/init.d/agentd: K10agentd`

The `S90agentd` link starts the service and the `K10agentd` link stops the service. The two-digit numbers in the links indicate the start and stop priorities of the service.

e) Use the `S90agentd` and `K10agentd` links to test starting and stopping the service. The links are called automatically when the system is booted or shut down.

See also

- *Starting and Stopping Sybase Control Center in Windows* on page 22
- *scc Command* on page 25

scc Command

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

Syntax

```
scc[.bat | .sh] [-a | --address RMI-service-address]
[-b | --bitwidth]
[-disable | --disable service-names]
[-enable | --enable service-names]
```

```
[-h | --help]
[-I | --info [information-category]]
[-m | --message message-level]
[-password | --password password]
[-p | -port | -ports | --port | --ports {port-name=port-number |
    service-name:property-name=port-number}]
[{-start | --start} | {-stop | --stop}]
[-status | --status]
[-user | --user login-name]
[-version | --version]
```

Parameters

- **-a | --address *RMI-service-address* –** the address for the RMI service to use; must be an IP address on this machine or the name of this machine (which is the default).
- **-b | --bitwidth –** returns a string identifying the bit width (32 or 64) of the underlying platform; Sybase Control Center uses this option to determine which libraries to use for its internal database. If you use this option, the **scc** command does not start Sybase Control Center.
- **-disable | --disable *service-names* –** disable the specified Sybase Control Center services. This option does not work while Sybase Control Center is running or as part of a start command. To use it, shut down SCC, execute `scc --disable`, then restart. Separate each service from the next with a comma.
- **-enable | --enable *service-names* –** enable the specified Sybase Control Center services. Separate each service from the next with a comma. If you use this option, **scc** does not start Sybase Control Center.
- **-h | --help –** display help and usage information for the **scc** command. If you use this option, **scc** does not start Sybase Control Center.
- **-I | --info [*information-category*] –** display the specified categories of information about Sybase Control Center. Separate each category from the next with a comma. The information categories are:
  - all – returns all the information provided by the sys, ports, and services categories. Default option.
  - sys – returns general information about this instance of Sybase Control Center, including the version, the home (installation) directory, the host machine's name and IP address, the RMI port number, the messaging level, and details about the platform and Java installation.
  - ports – lists all the ports on which the Sybase Control Center agent and its services listen, indicates whether each port is in use, and shows the service running on each port.
  - services – lists all the services known to the Sybase Control Center agent, indicates whether each service is enabled, and lists other services on which each service depends.
  - sysprop – lists all the Java system properties known the Java VM and their values.

  - env – lists the complete Java VM process environment.
- **-m | --message *message-level* –** set the amount of detail recorded in system logs; also known as the logging level. Valid values are OFF, FATAL, ERROR, WARN, INFO, DEBUG, and ALL. WARN is the default.
- **-password | --password –** specify the password of the user account Sybase Control Center will use to stop servers or query them for status. Use this option with **--user**. When you enter a command with **--user** but without **--password**, the console prompts you to enter a password.
- **-p | -port | -ports | --port | --ports {*port-name*=*port-number* | *service-name*:*property-name*=*port-number*} –** configure the specified service to run on the specified port. Changing ports is useful if you discover a port conflict between Sybase Control Center and other software on the same system. Valid port names, service names and property names are:

Short name	Description	Service names	Property names	Default port number
db	Database port	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	EmbeddedWebCon-tainer	http.port	8282
https	Web HTTPS (se-cure HTTP) port	EmbeddedWebCon-tainer	https.port	8283
jiniHttp	JINI HTTP server	Jini	httpPort	9092
jiniRmid	JINI Remote Meth-od Invocation dae-mon	Jini	rmidPort	9095
msg	Messaging port	Messaging	messaging.port	2000
rmi	RMI port	RMI	port	9999
tds	Tabular Data Stream™ port (used to communicate with other Sybase products)	Tds	tdsPort	9998

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

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

Examples

- **Example 1 –** both of these commands set the RMI port to 9999 (the default)

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

- **Example 2 –** this command sets all four of the SQL Anywhere database ports (data server, messaging, database alert, and scheduler) to 3638. (SQL Anywhere is the Sybase Control Center internal repository.)

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

- **Example 3 –** this command sets the TDS port to 9998

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

Permissions

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

See also

- *Starting and Stopping Sybase Control Center in Windows* on page 22
- *Starting and Stopping Sybase Control Center in UNIX* on page 23

Logging in to Sybase Control Center

Enter the Sybase Control Center Web console.

Prerequisites

- Install Adobe Flash Player in the browser you will use for Sybase Control Center. See the *Sybase Control Center Installation Guide* for details.
- You must be an authorized user to log in to Sybase Control Center.

Sybase Control Center is designed to delegate user authentication to the operating system or to an LDAP directory service. Consult your Sybase Control Center administrator if you are not sure which login account to use for Sybase Control Center.

1. In the Web browser, enter: `https://hostname:8283/scc`.
2. Enter your user name and password, and click **Login**.

Note: If you are using a Windows account to log in to Sybase Control Center, enter your user name in the format username@domain—for example, fred@sybase.

Logging out of Sybase Control Center

When you finish working in Sybase Control Center, exit the Web console.

From the main menu bar, select **Application > Logout.**

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

Note: If you leave your login session open on a screen that refreshes (a monitor screen or a data collection job screen, for example), the session remains open indefinitely. If you leave your session open on a screen that does not change, you will be logged out after 10 to 30 minutes.

User Authorization

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

Access to Sybase Control Center is controlled by login accounts. You grant permissions to a login account by assigning predefined roles that control tasks the user can perform in Sybase Control Center, such as administration and monitoring of particular types of Sybase servers. The roles can be assigned directly to login accounts or to groups; a login account inherits the roles of any group to which it belongs. Component product modules assign some roles automatically; see the help for your component for more information.

Sybase Control Center classifies roles as follows:

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

Assigning a Role to a Login or a Group

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

Prerequisites

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

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

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

   Note: Sybase Control Center product modules assign certain roles automatically, so you might not need to add a MonitorRole. See the help for your product module for more information.

   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 31
- *Adding a Group* on page 31
- *Removing a Group* on page 32
- *Adding a Login Account to a Group* on page 33
- *Removing a Login Account from a Group* on page 33
- *Adding a Login Account to the System* on page 34
- *Removing a Login Account from the System* on page 35
- *Modifying a User Profile* on page 36
- *Logins, Roles, and Groups* on page 37
- *Mapping Sybase Control Center Roles to LDAP or OS Groups* on page 19
- *User Authorization* on page 29

Removing a Role from a Login or a Group

Use the security configuration options to remove one or more roles from a Sybase Control Center login acount or from a group.

Prerequisites

You must have administrative privileges to perform this task.

1. From the menu bar, select **Application** > **Administration** .
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Click **Logins** or **Groups**.
4. Select the login account or group from which you want to remove a role.
5. Click the **Roles** tab.
6. Select the role, then click **Remove**.
7. Click **OK**.

See also

- *Assigning a Role to a Login or a Group* on page 30
- *Adding a Group* on page 31
- *Removing a Group* on page 32
- *Adding a Login Account to a Group* on page 33
- *Removing a Login Account from a Group* on page 33
- *Adding a Login Account to the System* on page 34
- *Removing a Login Account from the System* on page 35
- *Modifying a User Profile* on page 36
- *Logins, Roles, and Groups* on page 37

Adding a Group

Use the security configuration options to create a new group.

Prerequisites

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

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

1. From the main menu bar, select **Application** > **Administration** .
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Groups**.
4. Click **Create Group**.

5. Enter a group name and a description.
6. Click **Finish**.

See also

- *Assigning a Role to a Login or a Group* on page 30
- *Removing a Role from a Login or a Group* on page 31
- *Removing a Group* on page 32
- *Adding a Login Account to a Group* on page 33
- *Removing a Login Account from a Group* on page 33
- *Adding a Login Account to the System* on page 34
- *Removing a Login Account from the System* on page 35
- *Modifying a User Profile* on page 36
- *Logins, Roles, and Groups* on page 37

Removing a Group

Use the security configuration options to remove a group.

Prerequisites

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

1. From the main menu bar, select **Application** > **Administration** .
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Groups**.
4. Select the group to remove.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.

See also

- *Assigning a Role to a Login or a Group* on page 30
- *Removing a Role from a Login or a Group* on page 31
- *Adding a Group* on page 31
- *Adding a Login Account to a Group* on page 33
- *Removing a Login Account from a Group* on page 33
- *Adding a Login Account to the System* on page 34
- *Removing a Login Account from the System* on page 35
- *Modifying a User Profile* on page 36
- *Logins, Roles, and Groups* on page 37

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.

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

See also

- *Assigning a Role to a Login or a Group* on page 30
- *Removing a Role from a Login or a Group* on page 31
- *Adding a Group* on page 31
- *Removing a Group* on page 32
- *Removing a Login Account from a Group* on page 33
- *Adding a Login Account to the System* on page 34
- *Removing a Login Account from the System* on page 35
- *Modifying a User Profile* on page 36
- *Logins, Roles, and Groups* on page 37

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.

1. From the main menu bar, select **Application** > **Administration** .
2. In the Sybase Control Center Properties, expand the **Security** folder.
3. Select **Groups**.
4. Select the group from which to remove members.
5. Click the **Membership** tab.
6. Select the login, then click **Remove**.

7. Click **OK**.

See also

- *Assigning a Role to a Login or a Group* on page 30
- *Removing a Role from a Login or a Group* on page 31
- *Adding a Group* on page 31
- *Removing a Group* on page 32
- *Adding a Login Account to a Group* on page 33
- *Adding a Login Account to the System* on page 34
- *Removing a Login Account from the System* on page 35
- *Modifying a User Profile* on page 36
- *Logins, Roles, and Groups* on page 37

Adding a Login Account to the System

Use the security configuration options to create a new login account in Sybase Control Center.

Prerequisites

- You must have administrative privileges (sccAdminRole) to perform this task.
- If you intend to use Windows or UNIX to authenticate users, configure the appropriate authentication module.

1. From the main menu bar, select **Application** > **Administration** .
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Logins**.
4. Click **Create Login**.
5. Enter a login name and expiration for the new account. Expiration is optional.
6. Click **Next**.
7. Select **Specify new user information**.
8. Specify:
   - Title
   - First name*
   - Middle initial
   - Last name*
   - Suffix
   - Email address*
   - Phone
   - Ext.
   - Fax

- Mobile

*You must fill in the **First Name**, **Last Name**, and **Email Address** fields.

9. Click **Finish**.

Note: If you are using the predefined Simple Login module for authentication, the default login accounts, “sccadmin” and “sccuser,” come with blank passwords. To change or modify the passwords, configure the `csi.properties` file as described in the *Installation Guide*.

Next

Grant privileges to the new login account. You can grant privileges by assigning Sybase Control Center roles directly to the login accounts, or by assigning the login accounts to groups and mapping Sybase Control Center roles to the groups. The group approach is generally more efficient.

See also

- *Assigning a Role to a Login or a Group* on page 30
- *Removing a Role from a Login or a Group* on page 31
- *Adding a Group* on page 31
- *Removing a Group* on page 32
- *Adding a Login Account to a Group* on page 33
- *Removing a Login Account from a Group* on page 33
- *Removing a Login Account from the System* on page 35
- *Modifying a User Profile* on page 36
- *Logins, Roles, and Groups* on page 37

Removing a Login Account from the System

Use the security configuration options to delete a Sybase Control Center login account.

Prerequisites

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

1. From the main menu bar, select **Application** > **Administration** .
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Logins**.
4. Select the login to delete.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.

See also

- *Assigning a Role to a Login or a Group* on page 30
- *Removing a Role from a Login or a Group* on page 31
- *Adding a Group* on page 31
- *Removing a Group* on page 32
- *Adding a Login Account to a Group* on page 33
- *Removing a Login Account from a Group* on page 33
- *Adding a Login Account to the System* on page 34
- *Modifying a User Profile* on page 36
- *Logins, Roles, and Groups* on page 37

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.

1. From the main menu bar, select **Application** > **Administration.**
2. In the Sybase Control Center Properties dialog, expand the **Security** folder.
3. Select **Logins**.
4. Select the login account to modify.
5. Click the **General** tab.
6. To suspend this account, click **Login disabled**.
7. To set the date on which this account will stop working, click the calendar icon next to the **Expiration** field and select a data.
8. Click **Apply**.
9. Click the **User Info** tab.
10. Edit the user information.

    When this user configures e-mail alert subscriptions, Sybase Control Center automatically populates the subscription dialog with the e-mail address you enter here.
11. Click **Apply**.

See also

- *Assigning a Role to a Login or a Group* on page 30
- *Removing a Role from a Login or a Group* on page 31
- *Adding a Group* on page 31
- *Removing a Group* on page 32
- *Adding a Login Account to a Group* on page 33

Logins, Roles, and Groups

Sybase Control Center includes predefined login accounts and roles.

In Sybase Control Center, a login account identifies a user who can connect to the application. An account may have roles that specify the tasks the user is allowed to perform.

Sybase Control Center is designed to delegate user authentication to the operating system or to an LDAP directory service. Delegation requires some configuration, however, so Sybase Control Center comes with two predefined login accounts. Sybase recommends using the predefined accounts only for installing and setting up Sybase Control Center. These accounts are not intended for use in a production environment.

Table 5. Predefined accounts

Login name	Description
sccadmin	Can use all the administration features in Sybase Control Center
sccuser	Test account with no special privileges

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

Table 6. Predefined roles

Role	Description
sccUserRole	Provides nonadministrative access to Sybase Control Center. Required for every user.
sccAdminRole	Provides administrative privileges for managing Sybase Control Center.
aseMonitorRole*	Provides privileges to monitor the Adaptive Server environment.
iqMonitorRole*	Provides privileges to monitor the Sybase IQ environment.
repMonitorRole	Provides privileges to monitor the replication environment.
repAdminRole	Provides administrative privileges for managing the replication environment.

*These monitoring roles are assigned to users automatically by Sybase Control Center product modules; it is generally not necessary to assign them manually.

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

See also

- *Assigning a Role to a Login or a Group* on page 30
- *Removing a Role from a Login or a Group* on page 31
- *Adding a Group* on page 31
- *Removing a Group* on page 32
- *Adding a Login Account to a Group* on page 33
- *Removing a Login Account from a Group* on page 33
- *Adding a Login Account to the System* on page 34
- *Removing a Login Account from the System* on page 35
- *Modifying a User Profile* on page 36

Manage Sybase Control Center

Learn to administer data collection jobs, alerts, logs, views, perspectives, and other tools provided by Sybase Control Center.

For configuration instructions, including intitial set-up procedures for alerts and data collection jobs, see the Configure section of the help module for your Sybase Control Center component.

Job Scheduling

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

In Sybase Control Center, collection jobs provide the data that appears on monitoring screens and charts. A collection is a set of key performance indicators (KPIs). When the scheduler runs a collection job, it gathers the value of each KPI in the collection and tags the data with the date and time it was gathered. The data is stored in the repository and displayed. Each product module has predefined collections that you can schedule.

You can define schedules as one-time or repeating. You can modify the schedule for a job based on a number of attributes such as:

- Repeat interval
- Date
- Time

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

For more information:

- Each Sybase Control Center product module has a default collection that is scheduled automatically. For details, see the topic on data collections in the Configure section of the help for your product module.
- For instructions on scheduling a data collection job, see Setting Up Statistics Collection in the Configure section of the help for your product module.

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 **Stop** again to confirm.

See also

- *Deleting a Data Collection Job* on page 40
- *Resuming and Suspending a Data Collection Job* on page 40
- *Adding a New Schedule to a Job* on page 41
- *Modifying the Data Collection Interval for a Job* on page 42
- *Resuming and Suspending the Scheduler* on page 43
- *Viewing the Job Execution History* on page 43

Deleting a Data Collection Job

Use the Properties view for a resource to delete one or more data collection jobs.

1. In the Perspective Resources view, select the resource associated with the job and select **Resource > Properties.**
2. Select **Collection Jobs**.
3. Select the job and click **Delete**.
4. Click **OK** to confirm the deletion.

See also

- *Executing and Stopping a Data Collection Job* on page 39
- *Resuming and Suspending a Data Collection Job* on page 40
- *Adding a New Schedule to a Job* on page 41
- *Modifying the Data Collection Interval for a Job* on page 42
- *Resuming and Suspending the Scheduler* on page 43
- *Viewing the Job Execution History* on page 43

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 and:
   - To resume a job, click **Resume**.
   - To suspend a job, click **Suspend**, then click **Suspend** again to confirm the suspension.

See also

- *Executing and Stopping a Data Collection Job* on page 39
- *Deleting a Data Collection Job* on page 40
- *Adding a New Schedule to a Job* on page 41
- *Modifying the Data Collection Interval for a Job* on page 42
- *Resuming and Suspending the Scheduler* on page 43
- *Viewing the Job Execution History* on page 43

Adding a New Schedule to a Job

Use the Properties view for a resource to add more than one schedule to a 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:

Table 7. New schedule details

Field	Description
Name	Name for this schedule
Description	Description of this schedule
Start date	Date the job should start running
Time	Time the job should start running

6. Select one of:
   - **Run once**
   - **Repeat until**

     For **Repeat until**, specify these details:

Field	Description
Repeat interval	Interval, in seconds, between job executions to be added to the schedule

Field	Description
Repeat until	Date the job should stop running
Time	Time the job should stop running

- **Repeat indefinitely**

  For **Repeat indefinitely**, specify these details:

Field	Description
Repeat interval	Interval, in seconds, between job executions to be added to the schedule

7. Click **Apply**.

See also

- *Executing and Stopping a Data Collection Job* on page 39
- *Deleting a Data Collection Job* on page 40
- *Resuming and Suspending a Data Collection Job* on page 40
- *Modifying the Data Collection Interval for a Job* on page 42
- *Resuming and Suspending the Scheduler* on page 43
- *Viewing the Job Execution History* on page 43

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 collection folder and select a job.
5. On the **Schedule** tab, modify the Repeat interval field.
6. Click **Apply**.

See also

- *Executing and Stopping a Data Collection Job* on page 39
- *Deleting a Data Collection Job* on page 40
- *Resuming and Suspending a Data Collection Job* on page 40
- *Adding a New Schedule to a Job* on page 41
- *Resuming and Suspending the Scheduler* on page 43
- *Viewing the Job Execution History* on page 43

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.

1. From the main menu bar, select **Application > Administration.**
2. In the Sybase Control Center Properties dialog, select **Scheduler**.
3. Do one of the following:
   - To resume the scheduler, click **Resume**.
   - To suspend the scheduler, click **Suspend**.
4. Click **OK**.

See also

- *Executing and Stopping a Data Collection Job* on page 39
- *Deleting a Data Collection Job* on page 40
- *Resuming and Suspending a Data Collection Job* on page 40
- *Adding a New Schedule to a Job* on page 41
- *Modifying the Data Collection Interval for a Job* on page 42
- *Viewing the Job Execution History* on page 43

Viewing the Job Execution History

Use the Properties view to display a data collection job's execution history.

1. In the Perspective Resources view, select the resource associated with the job and select **Resource > Properties.**
2. Select **Collection Jobs**.
3. Select a job.
4. Click the **History** tab.

See also

- *Executing and Stopping a Data Collection Job* on page 39
- *Deleting a Data Collection Job* on page 40
- *Resuming and Suspending a Data Collection Job* on page 40
- *Adding a New Schedule to a Job* on page 41
- *Modifying the Data Collection Interval for a Job* on page 42
- *Resuming and Suspending the Scheduler* on page 43

Alerts

You can configure Sybase Control Center to notify you when a resource requires attention.

You do this by setting up a predefined alert that is triggered when a performance counter enters a particular state or passes a threshold value that you set. When the alert goes off, it generates an alert notification.

An alert notification takes the form of a visual indicator in the Alert Monitor and, optionally, an e-mail message. The Alert Monitor displays information about the alert, including the resource name, alert severity, value, and date. You can resolve the alert or allow it to escalate.

Configure, monitor, and control alerts for managed resources by:

- Enabling and disabling alert subscriptions for resources
- Configuring shell scripts to run when alerts fire
- Setting alert state or threshold triggers
- Responding to an alert by resolving it, adding notes if desired
- Modifying or deleting alerts
- Viewing alert history

Note: For instructions on creating alerts, see the Configuration section of the help for your Sybase Control Center product module.

Types, Severities, and States

Learn about the properties that define and control alerts.

An alert's type determines what causes it to fire.

Table 8. Alert types

Type	Description
State	A state alert fires when the metric on which it is based changes to a particular state. The possible states are running, pending, stopped, warning, error, and unknown.
Threshold	A threshold alert fires when the metric on which it is based passes a specified level.

Alert severities control when an alert is issued. You can configure the states or threshold values for each alert.

Table 9. Alert severities

Severity	Description
Normal	No alert is issued.
Warning	A problem has given cause for concern. An alert is issued; you can choose whether to subscribe to alerts that fire at the Warning level.
Critical	A serious problem exists. An alert is issued; you can choose whether to subscribe to alerts that fire at the Critical level.

State-based alerts use these states:

- Running
- Pending
- Unknown
- Warning
- Stopped
- Error

The definitions of these states vary by component and sometimes by alert. See the component-specific topics for details.

See also

- *Viewing Alerts* on page 45
- *Modifying an Alert* on page 46
- *Deleting an Alert* on page 46
- *Alert Subscriptions* on page 47
- *Alert Notifications* on page 49

Viewing Alerts

Display alert notifications and alerts that have been configured for a given resource.

- To display generated alerts (notifications):
  a) Select **View** > **Open** > **Alert Monitor** from the application menu bar.
  For a given alert, the Alert Monitor displays only the most recent unresolved notifications at each severity level. That is, if an alert fires five times at the warning level, only the notification of the fifth firing is listed—even if the previous four alerts remain unresolved.
  b) To display information about a generated alert, select the alert in the Alert Monitor and click **Properties**.
- To display configured alerts:

a) In the Perspective Resources view, select a resource and select **Resource** > **Properties.**
b) Click **Alerts** to view configured alerts for the selected resource.
(This is a different route to the information displayed in the second step, above.)

See also

- *Types, Severities, and States* on page 44
- *Modifying an Alert* on page 46
- *Deleting an Alert* on page 46
- *Alert Subscriptions* on page 47
- *Alert Notifications* on page 49

Modifying an Alert

Use the Properties view of your managed resource to modify an alert.

Note: To modify the configuration of storm suppression or alert-triggered scripts, delete the alert and recreate it.

1. In the Perspective Resources view, select a resource and select **Resource** > **Properties.**
2. Select **Alerts**.
3. Select the alert to modify.
4. On the Thresholds tab, modify the threshold values.
5. On the Subscriptions tab, select a subscription and click **Modify** to change its e-mail address or escalation address.
6. Click **Apply**.

See also

- *Types, Severities, and States* on page 44
- *Viewing Alerts* on page 45
- *Deleting an Alert* on page 46
- *Alert Subscriptions* on page 47
- *Alert Notifications* on page 49

Deleting an Alert

Use the Properties view of your resource to delete an alert.

1. In the Perspective Resources view, select a resource and select **Resource** > **Properties.**
2. Select **Alerts**.

3. Select an alert and click **Drop**.
4. Click **Yes** to confirm the deletion.

See also

- *Types, Severities, and States* on page 44
- *Viewing Alerts* on page 45
- *Modifying an Alert* on page 46
- *Alert Subscriptions* on page 47
- *Alert Notifications* on page 49

Alert Subscriptions

When an alert subscription is configured, the alert notifies the specified user or group of users by e-mail message when the alert fires.

You can configure an alert subscription to send e-mail notifications when the alert reaches a severity of warning, a severity of critical, or both.

You can also configure an alert subscription to escalate after a specified period of time. If the alert is not resolved within the time allowed, it e-mails an escalation message to the user or group whose address you provide. Sybase recommends that if you configure alert subscriptions to escalate, you do so only for the most urgent alerts, those with a severity of critical.

See also

- *Types, Severities, and States* on page 44
- *Viewing Alerts* on page 45
- *Modifying an Alert* on page 46
- *Deleting an Alert* on page 46
- *Alert Notifications* on page 49

Adding or Modifying an Alert Subscription

Use the Properties view to subscribe to an alert or edit an alert subscription.

Prerequisites

Specify the e-mail server to which Sybase Control Center will send e-mail alert notifications.

Each alert can support one subscription. To change addresses, modify the alert's existing subscription.

Note: E-mail notifications are sent from an address of the form SybaseControlCenter@yourdomain—for example, SybaseControlCenter@Bigcompany.com. Make sure your mail system does not block or filter that address.

1. In the Perspective Resources view, select a resource and select **Resource > Properties.**
2. Select **Alerts**.
3. Select an alert instance.
4. On the **Subscriptions** tab:
   - Click **Add** to create a subscription, or
   - Select a subscription and click **Modify** to edit an existing subscription
5. Follow the instructions in the Add Alert Subscription wizard.

   For both critical and warning alerts:

Table 10. Alert subscription details

Option	Description
E-mail message	To send an e-mail notification when this alert fires, click the **E-mail message** box and enter the e-mail address of one user or list.
Escalation e-mail	To escalate this alert (by sending an e-mail notification to another address when this alert has not been responded to after a specified period of time), click the **Escalation e-mail** box and enter the e-mail address of one user or list.
Time period	Enter the amount of time to wait, following the initial alert notification, before Sybase Control Center sends an e-mail notification to the escalation address.

6. Click **Finish**.

See also

- *Unsubscribing from an Alert* on page 48
- *Enabling and Disabling Alert Subscription* on page 49
- *Configuring the E-mail Server* on page 20

Unsubscribing from an Alert

Use the Properties view to unsubscribe from an alert.

1. In the Perspective Resources view, select a resource and select **Resource > Properties.**
2. Select **Alerts**.
3. Select an alert instance.
4. In the Subscriptions tab, select the alert subscription and click **Drop**.
   When you drop a regular subscription, any escalation subscription is also dropped. However, dropping an escalation does not affect the regular subscription.

5. Click **Yes** to confirm the deletion.

See also

- *Adding or Modifying an Alert Subscription* on page 47
- *Enabling and Disabling Alert Subscription* on page 49

Enabling and Disabling Alert Subscription

Use the Properties view to enable and disable alert subscription.

1. In the Perspective Resources view, select a resource and select **Resource > Properties.**
2. Select **Alerts**.
3. Select an alert instance.
4. In the **Subscriptions** tab, select an alert subscription and:
   - To enable subscription, click **Enable**.
   - To disable subscription, click **Disable**, then click **Yes** to confirm.

See also

- *Adding or Modifying an Alert Subscription* on page 47
- *Unsubscribing from an Alert* on page 48

Alert Notifications

An alert notification indicates that an alert has been generated.

Alert notifications are produced when alerts fire. An alert fires if the performance indicator on which it is based passes the threshold or state specified for the severity level of warning. If the performance indicator passes the threshold or state specified for the severity level of critical, the alert fires again and another notification is generated.

Detailed alert notifications appear in the Alert Monitor view. In addition, alerts appear as yellow ! symbols in the heat chart. You can set an alert to also send an e-mail message when it fires.

See also

- *Types, Severities, and States* on page 44
- *Viewing Alerts* on page 45
- *Modifying an Alert* on page 46
- *Deleting an Alert* on page 46
- *Alert Subscriptions* on page 47
- *Status Icons* on page 2

Displaying Alert History and Resolutions

Use the Properties view to see historical information about resolved and unresolved alerts.

The History tab on the Alerts page of the Resource Properties view displays information about every time this alert has fired. Each row of the table represents a single notification generated by the selected alert.

The Resolutions tab displays information about alerts that have been resolved (closed) by a Sybase Control Center administrator.

The History and Resolutions tabs display the 100 most recent alerts or alerts for the last 24 hours, whichever is reached first.

1. In the Perspective Resources view, select a resource and select **Resource > Properties.**
2. Select **Alerts**.
3. Select the alert instance.
4. Click the **History** tab.
5. (Optional) Click the **Resolutions** tab.

See also

- *Resolving Alerts* on page 50

Resolving Alerts

After you address the cause of an alert, resolve it to remove it from the list of active alerts in the Alert Monitor.

Prerequisites

You must be logged in as a user with Sybase Control Center administrative privileges (sccAdminRole) to resolve alerts.

1. In the Perspective Resources view, select a resource and select **Resource > Properties.**
2. In the left pane, select **Alerts**.
3. Select an alert instance in the top table.
4. Click **Resolve**.
5. Enter an explanation of how you resolved the alert.
6. Click **Submit**.
   The state of the alert (shown in the State column) changes to Normal. Notifications on this alert disappear from the Alert Monitor.

   Note: See the Resolutions tab for details on resolved alerts.

See also

- *Displaying Alert History and Resolutions* on page 50

Resources

In Sybase Control Center, a resource is a unique Sybase product component or subcomponent. A server is the most common managed resource.

Sybase products comprise many components, including servers, databases, devices, and processes. A managed resource is a product component or subcomponent that Sybase Control Center allows you to monitor and manage.

The Resource Explorer window lists resources that you have registered with Sybase Control Center. Resources are registered at the server or agent level; registering a server or agent also makes Sybase Control Center aware of any subcomponents. You can register resources individually or register by importing resources in a batch. For instructions on registering, see the Configuration section of the help for your product module.

Once server and agent resources are registered, add them to perspectives so you can monitor their availability and performance and manage the resources to meet your needs.

You can register resources one at a time or in groups. See the topics on registering and importing resources in the Configure section of the help for your product module.

See also

- *Common Display Options* on page 3

Unregistering a Resource

Remove a server or other resource from Sybase Control Center.

For instructions on registering individual resources or importing them in a batch, see the Configure section of the help for your product component.

1. In the Resource Explorer, select the resource you want to unregister.
2. Select **Resources** > **Unregister.**
3. Click **Yes** to confirm the removal.

See also

- *Adding a Resource to a Perspective* on page 52
- *Removing a Resource from a Perspective* on page 52
- *Searching for Resources in the Resource Explorer* on page 52

Adding a Resource to a Perspective

Add a resource to the current perspective.

Add a server or other resource to a perspective so you can monitor and manage it along with other resources in the same perspective.

1. From the Sybase Control Center toolbar, click the **Launch resource explorer** icon.
2. Select the resources to add to your perspective. Select multiple resources by pressing the **Ctrl** key while you select. Then perform one of these actions:
   - Select **Resources > Add Resources to Perspective.**
   - Drag and drop resources from the Resource Explorer onto the Perspective Resources view. You can select and drag multiple resources.

See also

- *Unregistering a Resource* on page 51
- *Removing a Resource from a Perspective* on page 52
- *Searching for Resources in the Resource Explorer* on page 52

Removing a Resource from a Perspective

Remove a resource from the current perspective.

1. In the Perspective Resources view, select a resource and select **Resource > Remove.**
2. Click **Yes** to confirm the removal.

See also

- *Unregistering a Resource* on page 51
- *Adding a Resource to a Perspective* on page 52
- *Searching for Resources in the Resource Explorer* on page 52

Searching for Resources in the Resource Explorer

Search for all your managed resources or narrow your search for a particular resource.

1. Click the **Launch Resource Explorer** icon.
2. If the Filter pane is not visible in the Resource Explorer window, select **View > Filter** from the view's menu bar.
3. Enter your search term in the **Filter string** field.

   The search term can be any string that appears in the tabular portion of the Resource Explorer, such as the name, or part of the name, of a server or a resource type (ASE Server, for example).

4. (Optional) Select a filtering setting:
   - **Match case** – search for resources whose displayed data includes the search term, including uppercase and lowercase letters; or
   - **Exact match** – search for resources whose displayed data includes an item identical to the search term.
5. (Optional) Select a column from the **Filter on** list to restrict your search to that column.

See also

- *Unregistering a Resource* on page 51
- *Adding a Resource to a Perspective* on page 52
- *Removing a Resource from a Perspective* on page 52

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.

A perspective is the main workspace in the Sybase Control Center window. 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.

One resource can appear in many perspectives.

See also

- *Common Display Options* on page 3

Creating a Perspective

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

1. From the application menu bar, select **Perspective > Create.**
2. Enter a name for your perspective. The name can contain up to 255 characters.
3. Click **OK**.

See also

- *Removing a Perspective* on page 54
- *Renaming a Perspective* on page 54

Removing a Perspective

Delete a perspective window.

1. Select the perspective tab you want to delete.
2. In the main menu bar, select **Perspective** > **Delete.**
   The selected perspective disappears. If there are other perspectives, Sybase Control Center displays one.

See also

- *Creating a Perspective* on page 53
- *Renaming a Perspective* on page 54

Renaming a Perspective

Change the name of your perspective.

1. Select the perspective tab you want to rename.
2. From the main menu bar, select **Perspective** > **Rename.** .
3. Enter the new name for your perspective.
4. Click **OK**.

See also

- *Creating a Perspective* on page 53
- *Removing a Perspective* on page 54

Views

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

Within the framework of the perspective, you use views to monitor and manage your resources. For example, using a view you can monitor the performance or availability of a managed resource. You can re-arrange, tile, cascade, minimize, maximize, and generally control the display of the views in your persective.

In Sybase Control Center, views are dynamic based on the managed resource selected. Each perspective includes these views:

- Perspective Resources
- 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.

Managing a View

Open, close, minimize, maximize, or restore a view in the current perspective.

You can:

Task	Action
Open a view	Do one of the following: • In the Perspective Resources view, right-click a resource and select the view to open. • In the application menu bar, select **View > Open** and choose a view.
Close a view	Select the view to close. In the application menu bar, select **View > Close.** You can also click the **X** in the view's upper right corner.
Maximize a view	Click the box in the view's upper right corner. The view enlarges to fill the entire perspective window. Click the box again to return the view to its former size.
Minimize a view	Click the _ in the view's upper right corner. The view shrinks to a small tab at the bottom of the perspective window.
Minimize all views	In the application menu bar, select **View > Minimize All Views.**
Restore a view	Click the box on the minimized tab to maximize the view. Click the box again to return the view to its former (smaller) size so you can see other views at the same time.
Bring a view to the front	In the application menu bar, select **View > Select** and choose the view you want from the submenu.

See also

- *Arranging View Layout in a Perspective* on page 55

Arranging View Layout in a Perspective

Use the view layout options to manage your perspective space.

Click one of these icons from the Sybase Control Center toolbar:

- **Cascade all open views**
- **Tile all open views vertically**
- **Tile all open views horizontally**

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

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

See also

- *Managing a View* on page 55

Repository

The Sybase Control Center embedded repository stores information related to managed resources, as well as user preference data, operational data, and statistics.

You can back up the repository database on demand, schedule automatic backups, restore the repository from backups, and configure repository purging options. Full and incremental backups are available. A full backup copies the entire repository. An incremental backup copies the transaction log, capturing any changes since the last full or incremental backup.

By default, Sybase Control Center saves backups as follows:

- Each full backup is stored in its own subdirectory in `<SCC-install-directory>/backup`.
- Each incremental backup is stored in a file in `<SCC-install-directory>/backup/incremental`.

Sybase recommends that you periodically move backup files to a secondary storage location to prevent the installation directory from becoming too large.

Scheduling Backups of the Repository

Configure full and incremental backups of the repository to occur automatically.

Prerequisites

Determine your backup strategy, including when to perform full backups and incremental backups. For example, you might schedule incremental backups every day and a full backup every Saturday.

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

A full backup copies the entire repository. An incremental backup copies the transaction log, capturing any changes since the last full or incremental backup.

1. From the main menu, select **Application** > **Administration.**
2. In the left pane, select **Repository**.
3. Click the **Full Backup** tab.
4. (Optional) To change the directory in which backups will be stored, click **Browse** and navigate to the desired directory.
5. Select **Schedule a Regular Backup**.
6. Specify the day you want scheduled backups to begin. Enter a **Start date** or click the calendar and select a date.

7. (Optional) Use the **Time** and **AM/PM** controls to specify the time at which backups occur.
8. Specify how often backups occur by setting the **Repeat interval** and selecting hours, days, or weeks.
9. (Optional) To purge the repository after each backup, select **Run a repository purge after the backup completes**.
10. If you include purging in the backup schedule, go to the **Size Management** tab and unselect **Automatically purge the repository periodically** to disable automatic purging.
11. Click **Apply** to save the schedule.
12. Click the **Incremental Backup** tab and repeat the steps above to schedule incremental backups to occur between full backups.

Next

Set purging options on the Size Management tab.

See also

- *Modifying the Backup Schedule* on page 57
- *Forcing an Immediate Backup* on page 58
- *Restoring the Repository from Backups* on page 58
- *Configuring Repository Purging* on page 60

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.

1. From the main menu, select **Application** > **Administration.**
2. In the left pane, select **Repository**.
3. Choose the type of backup to modify:
   - Click the **Full Backup** tab, or
   - Click the **Incremental Backup** tab.
4. (Optional) To suspend or resume the backup schedule, select or unselect **Schedule a Regular Backup**.
   When you unselect (uncheck) this option, the scheduling area is grayed out and scheduled backups no longer occur. However, the schedule is preserved and you can reinstate it at any time.
5. To change the backup schedule, edit the **Start date**, **Time**, **Repeat interval**, or units. You can also select or unselect **Run a repository purge after the backup completes**.
6. Click **Apply** to save the schedule.

See also

- *Scheduling Backups of the Repository* on page 56
- *Forcing an Immediate Backup* on page 58
- *Restoring the Repository from Backups* on page 58
- *Configuring Repository Purging* on page 60

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.

1. From the main menu, select **Application** > **Administration.**
2. In the left pane, select **Repository**.
3. Choose the type of backup to run:
   - Click the **Full Backup** tab, or
   - Click the **Incremental Backup** tab.
4. Click **Back up Now**.

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

See also

- *Scheduling Backups of the Repository* on page 56
- *Modifying the Backup Schedule* on page 57
- *Restoring the Repository from Backups* on page 58
- *Configuring Repository Purging* on page 60

Restoring the Repository from Backups

Load backup files into the repository database to revert undesirable changes or to recover from a catastrophic failure.

If you configured Sybase Control Center to store backups somewhere other than the default location, change the source directory in the copy commands in this procedure.

1. Shut down Sybase Control Center.
2. Copy the most recent full backup from `<SCC-install-directory>/backup/<generated_directory_name>` to `<SCC-install-directory>/services/Repository`. For example:

   Windows:

```
copy C:\sybase\SCC-3_1\backup\repository.
270110161105\scc_repository.db
C:\sybase\SCC-3_1\services\Repository
```

UNIX:

```
cp <SCC-install-directory>/backup/repository.270110161105/
scc_repository.db
<SCC-install-directory>/services/Repository
```

3. If you have no incremental backups to load,
   a) Also copy the log file from `<SCC-install-directory>/backup/<generated_directory_name>` to `<SCC-install-directory>/services/Repository`. For example:

      Windows:

      ```
      copy C:\sybase\SCC-3_1\backup\repository.
      270110161105\scc_repository.log
      C:\sybase\SCC-3_1\services\Repository
      ```

      UNIX:

      ```
      cp <SCC-install-directory>/backup/repository.270110161105/
      scc_repository.log
      <SCC-install-directory>/services/Repository
      ```

   b) Skip to step *5* on page 59.
4. 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 <SCC-install-directory>\services\Repository

   ..\SccSaDataserver\sa\bin_<platform>\dbsrv11.exe
   scc_repository -ad <SCC-install-directory>\backup\incremental
   ```

   UNIX:

   ```
   cd <SCC-install-directory>/services/Repository

   ../SccSaDataserver/sa/bin_<platform>/dbsrv11 scc_repository -ad
   <SCC-install-directory>/backup/incremental
   ```

   The repository database loads the full backup and any subsequent incremental backups present in the `incremental` directory. Incremental backups are loaded in date order. After loading and saving, the database shuts down.
5. Start Sybase Control Center.
   If you just loaded incremental backups, Sybase Control Center starts normally (that is, no further recovery occurs). If you copied a full backup to the `Repository` directory, the database recovers the repository from the full backup.

Example: Loading incremental backups into the repository database

These commands start SQL Anywhere on a 32-bit Windows machine:

```
% cd C:\sybase\SCC-3_1\services\Repository
% ..\SccSaDataserver\sa\bin_windows32\dbsrv11.exe
scc_repository -ad C:\sybase\SCC-3_1\backup\incremental
```

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

```
$ cd /opt/sybase/SCC-3_1/services/Repository
$ ../SccSaDataserver/sa/bin_aix64/dbsrv11 scc_repository -ad
/opt/sybase/SCC-3_1/backup/incremental
```

See also

- *Scheduling Backups of the Repository* on page 56
- *Modifying the Backup Schedule* on page 57
- *Forcing an Immediate Backup* on page 58
- *Configuring Repository Purging* on page 60
- *Starting and Stopping Sybase Control Center in Windows* on page 22
- *Starting and Stopping Sybase Control Center in UNIX* on page 23

Configuring Repository Purging

Change repository purging options.

Prerequisites

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

As you decide how to purge your repository, consider that:

- Purging keeps the repository from absorbing too much disk space.
- By default, purging is enabled. It occurs once a day and purges data older than one day.
- Statistics and alert history can help you detect trends in server performance and user behavior. The Sybase Control Center statistics chart can graph performance data over a period of a year or more if the data is available. If you have enough disk space, consider saving data for a longer period of time or disabling the purging of statistics or alert history.
- Changing the purge frequency and other options might affect Sybase Control Center performance.

Note: If you configure purging as part of a scheduled backup of the repository, disable automatic purging on the Size Management tab.

1. From the main menu bar, select **Application** > **Administration.**
2. Select **Repository**.
3. Click the **Size Management** tab.
4. To turn automatic purging on or off, click **Automatically purge the repository periodically**.

Turn this option off if purging is configured as part of your scheduled full or incremental backups.

5. Click purge options to turn them on or off:
   - **Purge statistics**
   - **Purge alert history**
6. In **Purge data older than**, enter the number of days after which to purge repository data.
7. Click **Apply**, then **OK**.

See also

- *Scheduling Backups of the Repository* on page 56
- *Modifying the Backup Schedule* on page 57
- *Forcing an Immediate Backup* on page 58
- *Restoring the Repository from Backups* on page 58

Logging

A log is a record of events related to a server or a client.

In Sybase Control Center, logging helps system administrators identify errors and other system events by recording messages about the events in log files. Sybase Control Center maintains these logs:

- The client log—captures messages about activities in the browser-based client components. These messages are generated by the component products 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 agent log, a composite log that records events in all components and in the Sybase Control Center framework
- The repository log—captures information about inserts and updates that have occurred in the Sybase Control Center repository, a SQL Anywhere database.

Viewing Sybase Control Center Server Logs

View event logs for the Sybase Control Center server.

Sybase Control Center logs events to several places:

- The console from which Sybase Control Center is launched.

- The Sybase Control Center agent log: `<SCC-install-directory>/log/agent.log`
- The repository log: `<SCC-install-directory>/log/repository.log`
- The component log for each installed Sybase Control Center product module. The path to the component log takes this form: `<SCC-install-directory>/plugins/<component>/log/<component>.log`

1. Display one of the log files using a log viewer or a method of your choice.
2. Look for entries of interest such as login attempts or the failure of a service to start.

   On the console and in the agent log file, some components prepend the component name to log entries.

See also

- *Viewing the Sybase Control Center Client Log* on page 62
- *Changing a Server's Logging Level* on page 62

Viewing the Sybase Control Center Client Log

Display the event log for the current session of your Sybase Control Center browser client.

In the perspective tab window (the main window), do either of the following to display the client log:

- Enter **Ctrl+Alt+L**.
- Select **View** > **Open** > **Log Window.**

Note: The client log reader displays the 100 most recent log messages for the current login session.

See also

- *Viewing Sybase Control Center Server Logs* on page 61
- *Changing a Server's Logging Level* on page 62

Changing a Server's Logging Level

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

If you are having a problem with Sybase Control Center, you might be able to discover the cause of the problem by changing the server logging level so that more events are recorded.

1. Shut down Sybase Control Center.
2. Restart Sybase Control Center using the -m option to change the logging level. In `<SCC-installation-dir>/bin`, enter:

   ```
   scc -m <logging-level>
   ```

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 rank.
FATAL	Logs only very severe error events that lead the server to abort.
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 rank.

3. Examine the server log for clues about what might be causing the problem.
4. When you have resolved the problem, set the logging level back to warn, the default. Your log may become unmanageably large if you leave it at the debug or all level.

Example

These commands, which must be executed in the installation directory, start Sybase Control Center with the logging level set to debug:

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

See also

- *Viewing Sybase Control Center Server Logs* on page 61
- *Viewing the Sybase Control Center Client Log* on page 62

Sybase Control Center Console

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

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

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

Console Commands

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

help Command

Display syntax information for one or more Sybase Control Center console commands.

Syntax

```
help [command_name]
```

Parameters

- **command_name –** optional. status, info, or shutdown. If you omit *command_name*, **help** returns information on all the console commands.

Examples

- **Example 1 –** returns information on the **status** command:

  ```
  help status
  ```

Permissions

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

See also

- *info Command* on page 64
- *shutdown command* on page 65
- *status Command* on page 66

info Command

Display information about specified parts of the Sybase Control Center server.

If you enter **info** with no parameters, it returns information for every parameter.

Syntax

```
info [-a | --sys]
[-D | --sysprop [system-property]]
[-e | --env [environment-variable]]
[-h | --help]
[-p | --ports]
[-s | --services]
```

Parameters

- **-a | --sys –** optional. List all the services known to the Sybase Control Center agent, 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 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.
- **-p | --ports –** optional. List all the ports on which the Sybase Control Center agent and its services listen, indicate whether each port is in use, and show the service running on each port.
- **-s | --services –** optional. List all Sybase Control Center services, indicate whether each service is enabled, and list other services on which each service depends.

Examples

- **Example 1 –** displays information about ports on this Sybase Control Center server:

```
info -p
```

Permissions

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

See also

- *help Command* on page 64
- *shutdown command* on page 65
- *status Command* on page 66

shutdown command

Stop the Sybase Control Center server if it is running.

Syntax

```
shutdown
```

Examples

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

```
shutdown
```

Permissions

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

See also

- *help Command* on page 64
- *info Command* on page 64
- *status Command* on page 66

status Command

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

Syntax

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

Parameters

- **-a | --agent –** display the status of the Sybase Control Center agent component.
- **-h | --help –** display information about the **info** command.
- **-p | --plugin [*plugin-name*] –** display the status of the specified Sybase Control Center plug-in (for example, ASEMap, the Adaptive Server management module). Omit the plugin-name argument to return a list of plug-ins.
- **-s | --service [*service-name*] –** display the status of the specified Sybase Control Center service (for example, the Alert service or the Messaging service). Omit the service-name argument to return a list of services.

Examples

- **Example 1 –** displays status information on the Repository service:

  ```
  status --service Repository
  ```

Permissions

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

See also

- *help Command* on page 64
- *info Command* on page 64
- *shutdown command* on page 65

Troubleshoot Sybase Control Center

Solve problems with core, shared features of Sybase Control Center.

See the help for your Sybase Control Center component for information on troubleshooting that component.

Cannot Log In

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

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

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

Ask the Sybase Control Center administrator to help you check.

See also

- *User Authorization* on page 29
- *Setting Up Security* on page 6

Sybase Control Center Fails to Start

Problem: The Sybase Control Center server does not start.

Solution: There might be a port conflict with another server. To check for port conflicts:

1. Execute this command:
   ```
   scc --info ports
   ```
   The command lists all the ports on which Sybase Control Center and its services listen, indicates whether each port is in use, and shows the service running on each port. If Sybase Control Center is not running, any port shown to be in use represents a conflict.
2. If you discover a conflict, use **scc --port** to change the port used by the Sybase Control Center service.

See also

- *scc Command* on page 25

Browser Refresh (F5) Causes Logout

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

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

Alerts Are Not Generated

Problem: Alerts are not being generated in Sybase Control Center.

Solution: Schedule a job to run the data collection that supports your alerts. See the data collections topic for your Sybase Control Center product module for information on which collections must be scheduled.

Performance Statistics Do Not Cover Enough Time

Problem: I want to graph performance counters over a long period of time but the statistics chart displays only very recent data.

Solution: Ask your Sybase Control Center administrator to change the repository purging options to keep statistical data available for as long as you need it. By default, statistics are purged frequently to conserve disk space.

See also

- *Configuring Repository Purging* on page 60

Index

A

B

C

D

E

F

G

R

S