



CHAPTER 14

Administration Tasks

This chapter explains administration tasks to be performed. It contains the following sections:

- [Manage Active Users and User Account, page 14-1](#)
- [Manage Control Center, page 14-2](#)
- [Manage TIBCO Rendezvous, page 14-7](#)
- [Manage Security, page 14-9](#)
- [User Access Log, page 14-26](#)

Manage Active Users and User Account

This section explains how to communicate with active users and manage the user account.

Active Users

Choose **Administration > Active Users > Active Users** and follow these steps:

-
- Step 1** After you choose **Administration > Active Users > Active Users**, a Active Users window appears that shows the currently logged users.
- Step 2** If you have the privileges of **SysAdmin** or **UserAdmin**, you can disconnect one or more users. Check the check box next to each user you want to disconnect. Then click the **Disconnect** button at the bottom of the window.



Caution

The current login sessions for the disconnected users are terminated and their work is lost.

- Step 3** To exit this list of all active users, choose another feature from the main product tabs.
-

User Account

Choose **Administration > Account > User Account** and follow these steps:

-
- Step 1** After you choose **Administration > Account > User Account**, a User Account window appears that shows the active users.
- Step 2** Click **Edit** to change the password, permissions, personal information, and user preferences.
- Step 3** Click **Save** to save the changes or click **Cancel**.
-

Manage Control Center

This section explains how to view and change the properties in the Dynamic Component Properties Library (DCPL); how to view status information about a host, servers, the WatchDog, and logs; how to define collection zones; and how to install license keys.

Choose **Administration > Control Center > Hosts** and you go to the default page of **Hosts**.

The Control Center Hosts window appears.

From **Administration > Control Center > Hosts**, you have the following choices:

- [Hosts, page 14-2](#)—**Hosts** allows you to manage the various servers.
- [Licensing, page 14-6](#)—**Licensing** is where you install license keys, which is the only way to access services and APIs.

Hosts

Choose **Administration > Control Center > Hosts**.

The Control Center Hosts window appears.



Note

Only the **Logs** buttons are enabled by default when there is no host selected. When the host is selected by checking the check box, the Logs buttons is disabled and the other buttons are enabled.

Click any of the buttons and proceed as follows:

- [Details, page 14-2](#)—Available only when the host system is chosen.
 - [Config, page 14-3](#)—Available only when the host system is chosen.
 - [Servers, page 14-4](#)—Available only when the host system is chosen.
 - [Watchdog, page 14-5](#)—Available only when the host system is chosen.
 - [Logs, page 14-5](#)—Available only when no host system selection is made.
-

Details

For details about a chosen host, follow these steps:

-
- Step 1** Choose a host by checking the check box to the left of the hostname and then click the **Details** button. You receive the Hosts Details window. This shows the details about the chosen host.

Step 2 Click **OK** and you return to Control Center Hosts window.

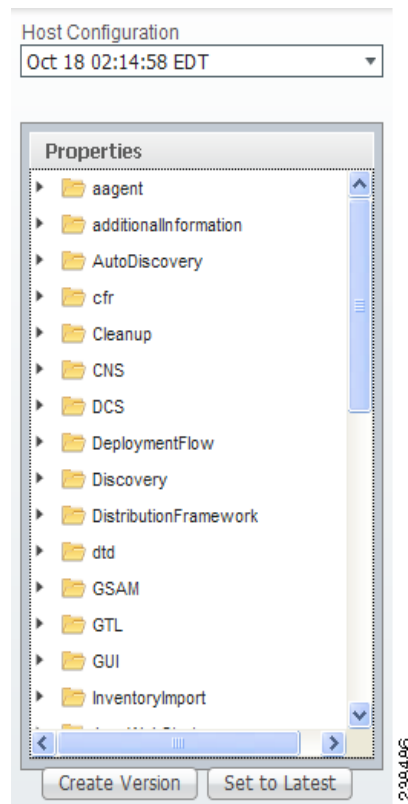
Config

To view or change the Dynamic Component Properties Library (DCPL) properties, follow these steps:

Step 1 From the Control Center Hosts window, check a check box next to a hostname for which you want to know the existing properties and then click the **Config** button.

A window as shown in [Figure 14-1](#), appears. It is a list of all the folders with all the properties. See [Appendix B, “Property Settings”](#) for a list of all the properties with explanations, defaults, and ranges/rules. If you do not know the property name, you can use a key word and do a Find on the pdf version of this appendix.

Figure 14-1 Properties

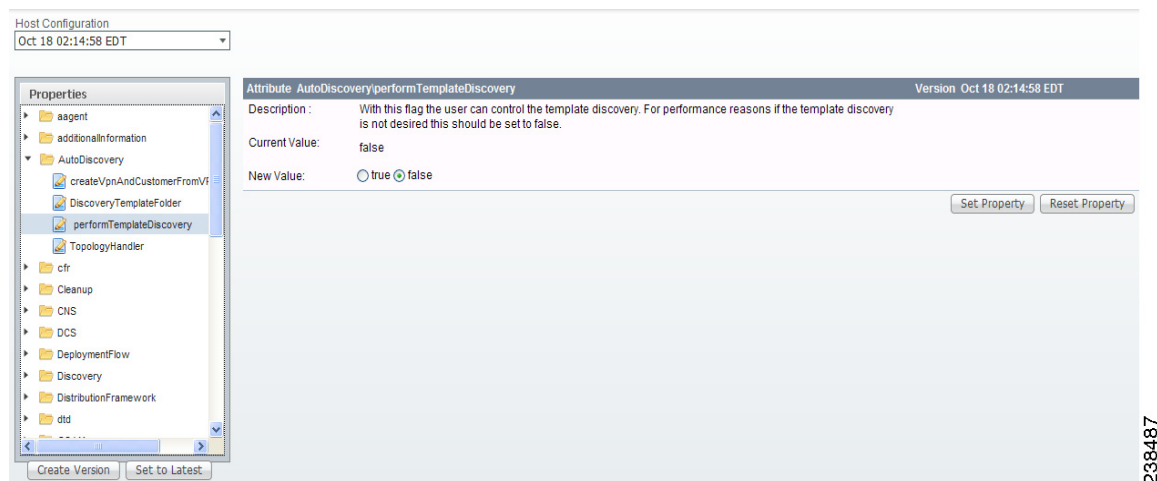


Step 2 Click the + sign to expand each folder.

The result could be more subfolders and the final level is the property name.

Step 3 Position the mouse over the folder or property name and you see a description.

Step 4 Click on an entry to get details and instructions on how to change the value, as shown in the example in [Figure 14-2](#).

Figure 14-2 Properties Detail Example

- Step 5** For each property that can be modified, you can modify the value and click **Set Property**. If when making your modifications, you want to return to the previous settings, click **Reset Property**.
- Step 6** After making all the changes you choose in each of the specific properties, you can click **Create Version** to create a new version of these properties. This feature gives you the option of saving multiple property sets for future use.
- Step 7** To view the values of previous versions of property sets, click the drop-down list in **Version** and select any version you choose.
- Step 8** When you click **Set to Latest** after selecting a version in [Step 7](#), this version is dated as the most current.
- Step 9** To return, click to the navigation path you want to use next.

Servers

To view the status information about the servers, follow these steps:

- Step 1** From the Control Center Hosts window, check a check box next to a hostname for which you want to know the server statistics and then click the **Servers** button.
- A window as shown in [Figure 14-3](#), appears.

Figure 14-3 Servers

#	<input type="checkbox"/> Name	State	Generation	Start Time	Successful Heartbeats	MissedHeartbeats
1	<input type="checkbox"/> nspoller	started	1	Oct 24 01:29:59 PM EDT	17682	0
2	<input type="checkbox"/> dbpoller	started	1	Oct 24 01:29:59 PM EDT	17830	0
3	<input type="checkbox"/> httpd	started	1	Oct 24 01:30:05 PM EDT	17703	0
4	<input type="checkbox"/> rgserver	disabled	10	Oct 24 01:38:29 PM EDT	0	0
5	<input type="checkbox"/> cnsserver	started	1	Oct 24 01:30:05 PM EDT	17645	0

Rows per page: 10 Page 1 of 1 Start Stop Restart Logs OK

- Step 2** Check any one check box next to the server you want to address and you have access to **Start**, **Stop**, **Restart**, and **Logs**. When you click on a specific server name or the Logs button, you get a list of server logs. If you then click on the log name for which you want details, the log viewer appears. You can filter this information in the log viewer. After you complete the task of your choice, you return to [Figure 14-3](#).
- Step 3** You can click a different server and click the button for the process of your choice. Or you can unclick the server choice and click **OK**.
- Step 4** After you click **OK** in [Figure 14-3](#), you return to the Control Center Hosts window.

Watchdog

To view the log information about WatchDog, follow these steps:

- Step 1** From the Control Center Hosts window, check a check box next to a hostname for which you want to know the WatchDog logs and then click the **Watchdog** button.
- A window as shown in [Figure 14-4](#), “**WatchDog Logs**,” appears.

Figure 14-4 WatchDog Logs

Name	Size	Last Modified
watchdog.0	768312	Friday, November 18, 2011 4:53:29 AM EST
watchdog.1	2000291	Thursday, November 17, 2011 10:28:12 PM EST

OK

- Step 2** Click on a specific WatchDog log name in the **Name** column to get the contents of that log. You can filter the information in this log. Click **OK** to return to [Figure 14-4](#).
- Step 3** You can repeat the process in [Step 2](#) or click **OK** to return to the Control Center Hosts window.

Logs

To view install and uninstall logs for the Master server, follow these steps:

-
- Step 1** From the Control Center Hosts window, be sure that no check boxes are checked.
- Step 2** Click the **Logs** drop-down list and select **Install** or **Uninstall**.
The window that appears is the log of installations or uninstallations, dependent on your selection in [Step 2](#).
- Step 3** Click the link in the **Name** column to view the detailed log information.
- Step 4** Click **OK** to return to the window.
- Step 5** Click **OK** again to return to the Control Center Hosts window.
-

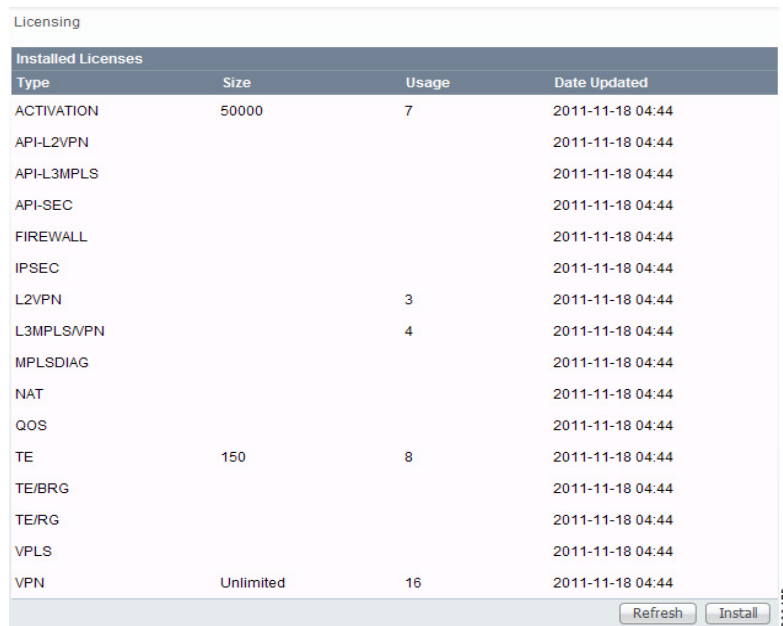
Licensing

Choose **Administration > Control Center > Licensing**.

To install license keys, follow these steps:

-
- Step 1** Choose **Administration > Control Center > Licensing**, and a window as shown in [Figure 14-5](#), appears.

Figure 14-5 Choose **Administration > Control Center > Licensing**



The screenshot shows a window titled "Licensing" with a table of installed licenses. The table has four columns: Type, Size, Usage, and Date Updated. The rows list various license types such as ACTIVATION, API-L2VPN, API-L3MPLS, API-SEC, FIREWALL, IPSEC, L2VPN, L3MPLS/VPN, MPLSDIAG, NAT, QOS, TE, TE/BRG, TE/RG, VPLS, and VPN. The Usage column shows values like 7, 3, 4, 8, and 16. The Date Updated column shows the date 2011-11-18 04:44 for all entries. At the bottom right of the table, there are "Refresh" and "Install" buttons.

Installed Licenses			
Type	Size	Usage	Date Updated
ACTIVATION	50000	7	2011-11-18 04:44
API-L2VPN			2011-11-18 04:44
API-L3MPLS			2011-11-18 04:44
API-SEC			2011-11-18 04:44
FIREWALL			2011-11-18 04:44
IPSEC			2011-11-18 04:44
L2VPN		3	2011-11-18 04:44
L3MPLS/VPN		4	2011-11-18 04:44
MPLSDIAG			2011-11-18 04:44
NAT			2011-11-18 04:44
QOS			2011-11-18 04:44
TE	150	8	2011-11-18 04:44
TE/BRG			2011-11-18 04:44
TE/RG			2011-11-18 04:44
VPLS			2011-11-18 04:44
VPN	Unlimited	16	2011-11-18 04:44

- Step 2** From the **Installed Licenses** table, click the **Install** button, as shown in [Figure 14-5](#). The Installed Licenses table explains the current statistics. The columns of information tell the **Type** of license keys you have installed (which can include ACTIVATION, API-L2VPN, API-L3MPLS, L2VPN, L3MPLS/VPN, MPLSDIAG, TE, TE/BRG, TE/RG, VPLS, VPN); the **Size**, which is valid for the **ACTIVATION** (licensed maximum global count of services), **TE** (number of TE-enabled nodes), or the **VPN** (maximum number of VPNs licensed); the **Usage**, which gives the number currently used for the rows; and the **Date Updated**, which reflects the refresh of the license usage (on an hourly basis, by default).

**Note**

When you purchase Traffic Engineering Management (TEM), you automatically receive **TE**, **TE/BRG**, and **TE/RG** licenses. All of these licenses *must* be installed to have access to all the Cisco Prime Fulfillment TEM features, including Planning Tools for protection planning (backup tunnels). The **TE** license serves as an activation license for the maximum number of TE-enabled nodes to be managed by TEM (you purchase licenses and upgrade licenses based on a range of nodes); the **TE/RG** license enables primary tunnel placement; and the **TE/BRG** license enables the Fast ReRoute (FRR) protection function.

**Note**

Click **Refresh** to give the most current status.

- Step 3** In the resulting Enter License Key window, enter a **License Key** that you received on your *Right to Use* paperwork with your product.

- Step 4** Click **Save**.

Your newly installed license appears in an updated version of the Installed License table, as shown in [Figure 14-5](#).

- Step 5** Repeat [Step 2](#), [Step 3](#), and [Step 4](#) for each of the *Right to Use* documents shipped with your product.

**Note**

When you receive multiple *Right to Use* documents to upgrade either the ACTIVATION License, which activates and sets the maximum global count of the services, or VPN licenses, which activates and set the maximum number of VPNs, be sure to enter the licenses in the correct order. For example, if you are upgrading from 500 to 3000 global count of the services and there are two steps to get there, enter the license to upgrade from 500 to 1500 and then the license key to upgrade from 1500 to 3000.

Manage TIBCO Rendezvous

The only reason you would ever use this functionality is if you change the TIBCO ports for TIBCO Rendezvous Agent (rva) or TIBCO Rendezvous Routing Daemon (rvrd) after installation. The changes being made here only affect the topology tool, a Java WebStart application.

Choose **Administration > Tibco > Tibco Manager** and follow these steps:

- Step 1** After you choose **Administration > Tibco > Tibco Manager**, a window appears as shown in [Figure 14-6](#).

Figure 14-6 TIBCO Rendezvous

General Information	
component:	rvrd
version:	8.2.2
license ticket:	346171
host name:	efgh-ultra
user name:	Unknown user
IP address:	10.10.10.124
client port:	7530
network services:	1
routing names:	0
store file:	/opt/PrimeFulfillment-6.2-M10/
process ID:	11965
managed:	no
control channel:	disabled
inbox port:	0

Step 2 From Figure 14-6, click **connection**, as described in Step 3; and click **change state**, as described in Step 4. These are choices in the left column of Figure 14-6.

Step 3 In Figure 14-6, when you click **connection**, a window appears as shown in Figure 14-7.

Figure 14-7 Connection Configuration

TIB/Rendezvous Daemon Connection:	
service:	7530
network:	
daemon:	

If you must change the **rva** port number from the existing value, change the **Accept Client Connections on Listen Port:** field to your new rva port number for Prime Fulfillment. If you must change the **rvrd** port number from the existing value, change the **service** field to your new rvrd port number for Prime Fulfillment. Then click **Submit**. Then Figure 14-7 returns with the new value and a note that says “Configuration change will take effect after RVA is re-activated. To re-activate RVA set it into idle state and then back to active state.”

Step 4 In Figure 14-6, click **change state**, follow the instructions, and you complete this functionality.

Step 5 From a terminal window, change to the **bin** directory of your Prime Fulfillment installation, such as `/opt/PrimeFulfillment/bin`.

Step 6 Source the Prime Fulfillment environment file in the `$PRIMEF_HOME/bin` directory:

- For K Shell or Bash - use the command `$PRIMEF_HOME/bin/vpnenv.sh`

Step 7 To start the script, at the command line type `updateWebStartJars`.

The next time you start a Java WebStart, such as the topology tool, these changes are in effect.

Manage Security

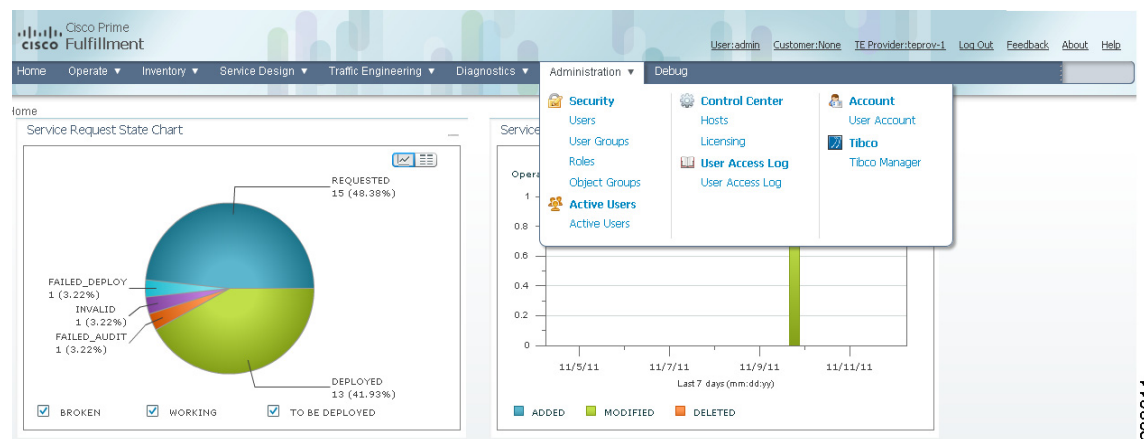
This section describes how system administrators create, edit, and delete users, user groups, user roles, and object groups and how privileges are assigned to these entities.

The security features are only accessible to the user **admin** or users with the following roles:

- **SysAdminRole**—Gives access to all the Prime Fulfillment tools. This is similar to “root” in a UNIX system.
- **UserAdminRole**—Gives access to only the user management tools.

Choose **Administration > Security** to access the user management tools. The window shown in [Figure 14-8](#), appears.

Figure 14-8 Administration, Security Window



You can choose one of the following options:

- [Users, page 14-9](#)—To manage users.
- [User Groups, page 14-14](#)—To manage user groups.
- [User Roles, page 14-16](#)—To manage user roles.
- [Object Groups, page 14-20](#)—To manage object groups.

For an example of how to use the Users, User Groups, User Roles, and Object Groups, see the “[User Roles Design Example](#)” section on [page 14-23](#).

Users

Choose **Administration > Security > Users** and the Users window appears.

The explanations of the buttons are given as follows:

- [Details, page 14-10](#)—View a User Detail Report
- [Create, page 14-10](#)—Create a new user
- [Copy, page 14-13](#)—Make a copy of an existing user and make changes to create a new user
- [Edit, page 14-13](#)—Edit selected user

- [Delete, page 14-13](#)—Delete selected user(s).
-

Details

When you click the **Details** button, located at the bottom of the Users window, you receive the following columns of information: **User ID**; **User Group** that a user belongs to; **Role** that a user occupies; **Resource Privilege** permissions that a user has for each role occupied; **Object Group** that a user role is associated with; **Customer View** that a user's role is limited to; **Provider View** that a user's role is limited to.

Create

When you click the **Create** button, located at the bottom of the Users window, a user with the required privileges can create a new user. Follow these steps:

- Step 1** Choose **Administration > Security > Users**.
- Step 2** Click the **Create** button and the window shown in [Figure 14-9](#), appears.

Figure 14-9 Create/Copy/Edit Users Window

Create New User

Security

User ID*:

Password*:

Verify Password*:

Permissions for Others: ☒ View ☒ Edit ☐ Delete

User Groups:

Assigned Roles:

Personal Information

Full Name*:

Work Phone:

Mobile Phone:

Pager:

Email:

Location:

Supervisor Information:

User Preferences

Rows per page:

Logging Level:

Step 3 Enter information in the **Security** section, as follows:

- **User ID** (required)—Enter a User ID for this new user.
- **Password** (required)—New password to replace any existing password:
 - Prime Fulfillment requires a non-blank password.
 - Prime Fulfillment passwords must be a minimum of five characters and no practical maximum length.
 - Prime Fulfillment does not employ any password restrictions or complexity rules; use good judgment in determining passwords.
 - Prime Fulfillment passwords are encrypted when stored in the repository.
 - Prime Fulfillment passwords do not expire.
 - Prime Fulfillment monitors inactivity and auto-logoff per the settings defined in the Dynamic Component Properties Library (DCPL) properties for **repository/rbac**, see [Appendix B, “Property Settings.”](#)
- **Verify Password** (required)—Confirm by re-entering the selected password.

- **Permission for Others**—Check each of the associated check boxes for the permission that the user (to be created) wants to give to other users. The user who creates the object is the owner of the objects. The creator can allow or disallow other users to **View**, **Edit**, and/or **Delete** the objects owned by the creator by defining permissions. This is the last line of defense. For UserA to delete an object X that UserB created, UserA must first have Delete permission for object X, then UserB's settings for permissions for others is checked, to finally decide whether UserA can delete object X. Permission for others can be enabled or disabled by setting the property: **repository.rbac.checkCreatorPermissionEnabled**. After you make a change, you must restart the WatchDog by entering **stopwd** followed by **startwd**. For more WatchDog details, see [Appendix C, "WatchDog Commands"](#).

- **User Groups**—Click **Edit** and you receive a list of the groups. Add this user to a user group(s). The user inherits all the roles assigned to the group(s). You can filter this list. From the selected groups, check the check box next to each group to which you want to add this user. Then click **OK**. You can repeat this procedure if you want to change your selection.

A user's group membership can also be changed in the group editor (see the ["Edit" section on page 14-15](#)).

- **Assigned Roles**—Click **Edit** and you receive a list of the roles. You can filter this list. From the selected roles, check the check box next to each role to which you want to assign this user. Then click **OK**. You can repeat this procedure if you want to change your selection.

The user inherits all the privileges from the groups in which it participates and from the roles assigned to it. That is, the permissions received by the user is an OR result of the permissions in each role.

Step 4 Enter information in the **Personal Information** section, as follows:

- **Full Name** (required)—Click the drop-down list and select a title; enter the first name; and then enter the last name.
- **Work Phone** (optional)—Enter the work phone number.
- **Mobile Phone** (optional)—Enter the **user's cell phone or mobile phone number**.
- **Pager** (optional)—Enter the user's pager number.
- **Email** (optional)—Enter the user's e-mail address.
- **Location** (optional)—Enter the user's location.
- **Supervisor Information** (optional)—Enter information about the supervisor.

Step 5 Enter information in the User Preferences section, as follows:

- **Language** (optional)—Click the drop-down list to select a language (at this time only English is supported).
- **Rows per page** (optional)—This defines the number of rows per page for object listing. The default is **10**. The choices are: **5, 10, 20, 30, 40, 50, 100, 500, 1000, and 2500**.
- **Logging Level** (optional)—The default is **Warning**. The choices are: **Off, Severe, Warning, Config, Info, Fine, Finer, Finest, and All** (see all levels of logs). This defines the logging level for viewing logging events. The list progresses from the least number of messages to the most number of messages.
- **Initial Screen** (optional)—The default is **Home**. The choices are: **Home, Service Inventory, Service Design, Monitoring, Administration, Site Index, and Diagnostics**. This is a way to specify the first window you will see after logging in.

Step 6 Click **Save**.

The Users window reappears with the new user listed.

Copy

The **Copy** button, located at the bottom of the Users window, provides a convenient way to create a new User by copying the information for an existing User including User Groups, Assigned Roles, and User Preferences. Follow these steps:

-
- Step 1** Choose **Administration > Security > Users**.
 - Step 2** Check one check box for the existing User you want to copy and edit to create a new User.
 - Step 3** Click the **Copy** button and the window shown in [Figure 14-9](#), appears.
Required entries are a **User ID**, **Password**, **Verify Password**, and **Full Name**.
 - Step 4** Make all the other changes you want by following the instructions in the [“Create” section on page 14-10](#).
 - Step 5** Click **Save** and you will return to the Users window.
The newly created **User** is added to the list and a Status Succeeded message appears in green.
-

Edit

The **Edit** button, located at the bottom of the Users window, allows a user with the required privileges to edit user-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > Users**.
 - Step 2** Check the check box for the row of the user you want to edit.
 - Step 3** Click the **Edit** button and a window as shown in [Figure 14-9](#), appears.



Note

To change your password without the SysAdmin or UserAdmin privileges, click the **Account** tab on the top of the Home page. This allows the user to edit the user profile, including changing the password.

- Step 4** Enter the desired information for the user profile, as specified in the [“Create” section on page 10](#).
 - Step 5** Click **Save**.
The Users window reappears with the edited user listed.
-

Delete

The **Delete** button, located at the bottom of the Users window, allows a user with the required privileges to delete user-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > Users**.
 - Step 2** Check the check box(es) for the row(s) of the user(s) you want to delete.

- Step 3** Click the **Delete** button and a confirmation window appears.
- Step 4** Click **Delete** to continue with the process of deleting information for the specified user(s). Otherwise click **Cancel**.
- The Users window reappears. If this was successful, the newly updated information appears and a **Status** box appears in the lower left corner of the window with a green check mark for **Succeeded**.

User Groups

A user group is a logical grouping of users with common privileges. The **User Groups** feature is used to create, edit, or delete user groups.

To access the User Groups window, choose **Administration > Security > User Groups**. The User Groups window appears.

The explanations of the remainder of the buttons is given as follows:

- [Create, page 14-14](#)—Create a new user group
- [Edit, page 14-15](#)—Edit selected user group
- [Delete, page 14-15](#)—Delete selected user group(s)

Create

The **Create** button, located at the bottom of the User Groups window, allows a user with the required privileges to create a user group. Follow these steps:

- Step 1** Choose **Administration > Security > User Groups**.
- Step 2** Click the **Create** button and the window shown in [Figure 14-10](#), appears.

Figure 14-10 Create/Edit User Groups Window

- Step 3** Enter information for the user group profile, as follows:
- **Name** (required)—Enter a name for the new user group.

- **Description** (optional)—Enter a description of this new user group.
- **Roles**— This allows you to assign roles to this user group. Click **Edit** and you receive a list of the roles. You can filter this list. From the selected roles, check the check box next to each role you want to attach to this user group. Then click **OK**. You can repeat this procedure if you want to change your selection.
- **Users**—This allows you to add users to this user group. Click **Edit** and you receive a list of the users. You can filter this list. From the selected users, check the check box next to each user you want to attach to this user group. Then click **OK**. You can repeat this procedure if you want to change your selection.

Step 4 Click **Save**. The User Groups window reappears with the new user group listed.

Edit

The **Edit** button, located at the bottom of the User Groups window, allows a user with the required privileges to edit user group-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > User Groups**.
- Step 2** Check the check box for the row of the user group you want to edit.
- Step 3** Click the **Edit** button and a window as shown in [Figure 14-10](#), appears.
- Step 4** Enter the desired information for the user group profile, as specified in [Step 3](#) of the “**Create**” section on [page 14-14](#).
- Step 5** Click **Save**.
- The User Groups window reappears with the edited user group list.
-

Delete

The **Delete** button, located at the bottom of the User Groups window, allows a user with the required privileges to delete user group-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > User Groups**.
- Step 2** Check the check box(es) for the row(s) of the user group(s) you want to delete.
- Step 3** Click the **Delete** button and a confirmation window appears.
- Step 4** Click **Delete** to continue the process of deleting information for the specified user group(s). Otherwise click **Cancel**.
- The User Groups window reappears. If this was successful, the newly updated information appears and a **Status** box appears in the lower left corner of the window with a green check mark for **Succeeded**.
-

User Roles

A user role is a predefined or a user-specified role defining a set of permissions. The **User Roles** feature is used to create, edit, or delete user roles.

To better understand the way roles are managed, certain specific characteristics of roles are defined as follows:

- **Parent Role**—All permission of the parent roles are inherited by the role that is being created or edited (child role). A child role always has the same or more privileges than its parent role.
- **Customer**—If a role is associated with a customer, a user of this role does not have access to the objects associated with other customers. Object types that are constrained by customer view are: Persistent Task, Customer Site, VPN, CPE, SR, Policy, Service Order, and resource pools that are associated with a Customer, Customer Site, or VPN.
- **Provider**—If a role is associated with a provider, a user of this role does not have access to the objects associated with other providers. Object types that are constrained by provider view are: Persistent Task, Access Domain, Region, PE, Policy, and some resource pools that are associated with a provider, Access Domain, Region, or PE.

Customer view and provider view within a role have no affect on those objects that do not belong to either a customer or a provider. Those object types are: task, probe, workflow, device, Prime Fulfillment host, and template.

Permission operation types in a Role editor, namely View, Create, Edit, and Delete mean View, Create, Modify, and Delete a database object. For example, SR modification (or subsumption) is viewed as Role Based Access Control (RBAC) Creation. SR purge is viewed as RBAC Delete.

A Role can be enabled to be associated with Object Group(s). When Object Group association is enabled, a Role can no longer be associated with a Customer or a Provider, and it cannot have a Parent Role. Resources are limited to PE, CPE, and Named Physical Circuit only. PE and CPE permission implies Device Permission.



Note

A global policy, the one that is not associated with any customer or provider, is accessible by both customer-view roles and provider-view roles.

Separate provider-view from customer-view roles when defining a role. When a role is associated with a provider, choose only the resources for which an access scope can be constrained by a provider view. Do the same for a customer-view role.

To access the User Roles window, choose **Administration > Security > Roles**. The User Roles Administration window appears.

The predefined roles are provided with associated permissions that cannot be edited or deleted. They are intended to cover most of the needed use cases to facilitate a rapid assignment of roles to users and groups with minimum manual configuration. They can also be used as examples to create new roles.

The explanations of the buttons is as follows:

- [Create, page 14-17](#)—Create a new user role
- [Copy, page 14-19](#)—Copy selected user role
- [Edit, page 14-20](#)—Edit selected user role
- [Delete, page 14-20](#)—Delete selected user role(s)

Create

The **Create** button, located at the bottom of the User Roles Administration window, allows a user with the required privileges to create a new user role. Follow these steps:

- Step 1** Choose **Administration > Security > Roles**.
- Step 2** Click the **Create** button and a window comprised of [Figure 14-11](#) and [Figure 14-12](#), appears.

Figure 14-11 Create/Copy/Edit User Roles Window (Top)

Create New Role

General Information

Name*:

Enable Object Group Association: ☐

Parent Role:

Customer:

Provider:

Object Groups:

Description:

Users:

User Groups:

238499

Figure 14-12 Create/Copy/Edit User Roles Window (Bottom)

Resource	All	Create	View	Modify	Delete
Persistent Task	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SAA Probe	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Workflow	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ISG Host	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Provider	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CPE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MPLS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MPLS Service Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
L2VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
L2VPN Service Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firewall Policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firewall Service Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NAT Service Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPsec Policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPsec Service Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Deployment Flow	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Template	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TE Provider	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TE Router	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TE Tunnel Policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TE Tunnel & Resource Service Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TE Traffic Admission Service Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPLS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPLS Service Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Service Order	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Object Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Named Physical Circuit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Diagnostics, L3VPN - CE to CE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MPLS Diagnostics Expert Console Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Discovery Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Staging Service Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Route Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Diagnostics, L3VPN - PE to PE (in VRF)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Diagnostics, L3VPN - PE to PE (Core)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Diagnostics, L3VPN - CE to PE across Core	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Diagnostics, L3VPN - PE to attached CE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Associate Template	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Datatile	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MPLS-TP Service Request	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MPLS-TP Policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note: * - Required Field

Save Cancel 238500

- Step 3** Enter the following information in [Figure 14-11](#):
- **Name** (required)—Enter the name of this new user role.
 - **Enable Object Group Association**—The default is that this check box is unchecked. In this case, **Parent Role**, **Customer**, and **Provider** are enabled and **Object Groups** is not enabled. A complete list of resources appears, as shown in the example in the User Roles Administration window. If you

check this check box, **Parent Role**, **Customer**, and **Provider** are not enabled and **Object Groups** is enabled. A window, as shown in [Figure 14-12](#), is reduced to just **PE**, **CPE**, and **Named Physical Circuit**.

- **Parent Role** (optional)—Click **Edit** and a list of the existing roles appears, similar to the User Roles Administration window, from which you can click the radio button for the parent role you choose. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no parent selection.
- **Customer** (optional)—Click **Edit** and a list of the existing customers appears. You can filter this list. From the selected customers, click the radio button for the customer you want to select to own this role. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no customer selection.

**Note**

A customer can only be associated with a logical device, such as **CPE** and **PE**. This is not possible with a physical device, such as **device**.

- **Provider** (optional)—Click **Edit** and a list of the existing providers appears. You can filter this list. From the selected providers, click the radio button for the provider you want to select to own this role. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no provider selection.
- **Object Groups** (optional)—Click **Edit** and a list of the existing object groups appears. You can filter this list. From the selected object groups, check the check box(es) for the object group(s) you want to associate with this User Role. Then click **OK**. You can repeat this procedure if you want to change your selection. Deselect the **Enable Object Group Association** button if you want no object group selection.
- **Description** (optional)—Enter the descriptive information about permissions in this field, as shown in the Description column of the User Roles Administration window.
- **Users** (optional)—Click **Edit** and a list of the existing users appears. You can filter this list. From the selected users, check the check box(es) for the user(s) you want assigned to this role. Then click **OK**. You can repeat this procedure if you want to change your selection.

**Note**

A user who is associated with a specific role cannot see objects associated with other customers or with other providers.

- **User Groups** (optional)—Click **Edit** and a list of the existing user groups appears. You can filter this list. From the selected user groups, check the check box(es) for the user group(s) you want assigned to this role. Then click **OK**. You can repeat this procedure if you want to change your selection.

Step 4 In [Figure 14-12](#), click any combination of the following permissions: **Create**; **View**; **Modify**; **Delete**. If you want all the permissions, click **All**.

**Note**

Prime Fulfillment Host refers to **Administration > Control Center > Hosts**. Here, you can view host details, perform configuration tasks, start and stop servers, activate a watchdog, and so on.

**Note**

SAA Probe is intended for management of SLA under **Inventory > Device Tools > SLA**. Any user who wants to generate SLA reports *must* have **View** permission on **Prime Fulfillment Host** in addition to **View** permission on **SAA Probe**.

**Note**

The **Workflow** object is currently not used.

**Note**

Template controls the template manager functions and **Associate Template** controls the ability to associate templates with service requests. If you choose **Create** permission in **Template**, you also automatically receive **Modify** permission. If you choose any or all permissions in **Associate Template**, you automatically turn on the **View** permission in **Template**.

**Note**

Datafile permission allows you to manage datafiles and list all Service Requests associating the datafile. If you choose any or all permissions in **Datafile**, you automatically turn on the **View** permission in **Template**.

Step 5 Click **Save**.

The User Roles Administration window reappears with the new user role listed.

Copy

The **Copy** button, located at the bottom of the User Roles Administration window, provides a convenient way to copy the information from an existing User Role and edit it to create a new User Role. Follow these steps:

**Note**

All fields in the existing role are copied to the new role, even including Users and User Groups. You should edit the new role *carefully* to reflect your intention.

Step 1 Choose **Administration > Security > Roles**.

Step 2 Check one check box for the existing User Role you want to copy and edit to create a new User Role.

Step 3 Click the **Copy** button and the window comprised of [Figure 14-11](#) and [Figure 14-12](#) appears.

Step 4 The required entry is a **Name**. A default name is given, **Copy of** and the name of the original User Role. You cannot duplicate a **Name**.

Step 5 Make all the other changes you want by following the instructions in the “[Create](#)” section on [page 14-17](#).

Step 6 Click **Save** and you will return to the User Roles Administration window.

The newly created **User** is added to the list and a Status Succeeded message appears in green.

Edit

The **Edit** button, located at the bottom of the User Roles Administration window, allows a user with the required privileges to edit user role-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > Roles**.
 - Step 2** Check the check box for the row of the user role you want to edit.
 - Step 3** Click the **Edit** button and a window appears combining [Figure 14-11](#) and [Figure 14-12](#) for this user role.
 - Step 4** Enter the desired information for the user role profile, as specified in [Step 3](#) and [Step 4](#) of the “[Create](#)” [section on page 14-17](#).
 - Step 5** Click **Save**.

The User Roles Administration window reappears with the edited user roles listed.

Delete

The **Delete** button, located at the bottom of the User Roles Administration window, allows a user with the required privileges to delete user role-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > Roles**.
 - Step 2** Check the check box(es) for the row(s) of the user role(s) you want to delete.
 - Step 3** Click the **Delete** button and a confirmation window appears.
 - Step 4** Click **Delete** to continue with the process of deleting information for the specified user role(s).

The User Roles Administration window reappears. If this was successful, the newly updated information appears and a Status box appears in the lower left corner of the window with a green check mark for **Succeeded**.

Otherwise click **Cancel**.

Object Groups

An Object Group is a named aggregate entity comprised of a set of objects. The object types can be PE, CE, Named Physical Circuit (NPC), and interfaces of PEs or CEs. An Object Group provides instance level of access granularity for users.

An Object Group can be associated with different roles. A role can be associated with an Object Group or it can be associated with a grouping of Customer and Provider, but it cannot be associated with both of these. The association with a grouping of Customer and Provider is either with Customer(s), with Provider(s), or with Customer(s) and Provider(s). When a role is associated with Object Group(s), you can only define permissions for PE, CE, and NPC. Permissions on interfaces is implied PEs or CEs, that is, PE Create or CE Create implies Interface Create. PE or CE Edit implies Interface Create, Edit, or Delete. CE or PE Delete implies Interface Delete.

When instance level of access is desired for PE, CE, NPC, or interface of PEs and CEs, you can usually define a role associated with Object Group(s) that contains a collection of PEs and CEs you are limited to operate. Then define other roles to include permissions on other types of objects. See the “[User Roles Design Example](#)” section on page 14-23.

If an Object Group contains PEs (or CEs) only, with no explicit interface as a group member, you can access all interfaces of grouped PEs or CEs. If an Object Group contains any explicit interface as group members, every single interface that you want to access you must manually choose to include as group members.

**Note**

Permissions are the union of all roles that you occupy. If your intention is to limit access to a scope of devices or Named Physical Circuits (NPCs), define a role to be associated with Object Group(s), Device, CE, PE, and NPC.

To access the Object Groups window, choose **Administration > Security > Object Groups**. The Object Groups window appears.

The explanations of the buttons is as follows:

- [Create, page 14-17](#)—Create a new object group
- [Edit, page 14-20](#)—Edit a selected object group
- [Delete, page 14-20](#)—Delete selected object group(s)

Create

The **Create** button, located at the bottom of the Object Groups window, allows a user with the required privileges to create a new object group. Follow these steps:

- Step 1** Choose **Administration > Security > Object Groups**.
- Step 2** Click the **Create** button and the window appears as shown in [Figure 14-13](#).

Figure 14-13 Create/Edit Object Group Window

- Step 3** Enter the following information in [Figure 14-13](#):

- **Name** (required)—Enter the name of this new object group.

- **Description** (optional)—Enter a description of this new object group.
- **PE Group Members** (optional)—Click **Edit** and a list of the existing PEs appears. You can filter this list. From the selected PEs, check the check box(es) for the PE(s) you want to include in this group. Then click **OK**. You can repeat this procedure if you want to change your selection(s). The **Interface Members** column will be empty. All existing interfaces for each of the PE Groups in the **Name** column will default to be members of the group unless you select only a subset. To limit the interfaces and select a subset of interfaces, click a PE Group in the **Name** column. You receive a list of all the interfaces for that PE from which you can individually select only the interfaces you want to associate with that PE Group. Then click **OK**. You return to [Figure 14-13](#) and the **Name** and selected **Interface Members** for each PE Group Member appear. If no entries exist in the **Interface Members** column for both **PE Group Members** and **CE Group Members**, the default is all existing interfaces for both (if any exist).
- **CE Group Members** (optional)—Click **Edit** and a list of the existing CEs appears. You can filter this list. From the selected CEs, check the check box(es) for the CE(s) you want to include in this group. Then click **OK**. You can repeat this procedure if you want to change your selection(s). The **Interface Members** column is empty. All existing interfaces for each of the CE Groups in the **Name** column default to be members of the group unless you select only a subset. To limit the interfaces and select a subset of interfaces, click a CE Group in the **Name** column. You receive a list of all the interfaces for that CE from which you can individually select only the interfaces you want to associate with that CE Group. Then click **OK**. You return to [Figure 14-13](#) and the **Name**, and selected **Interface Members** for each CE Group Member appear. If no entries exist in the **Interface Members** column for both **CE Group Members** and **PE Group Members**, the default is all existing interfaces for both (if any exist).
- **NPC Group Members** (optional)—Click **Edit** and a list of the existing NPCs appears. You can filter this list. From the selected NPCs, check the check box(es) for the NPC(s) you want to select to own this role. Then click **OK**. You can repeat this procedure if you want to change your selection(s). You return to [Figure 14-13](#) and the **Name** for each NPC Group Member appears.

Step 4 Click **Save**.

[Figure 14-13](#) reappears with the new object group listed.

Edit

The **Edit** button, located at the bottom of [Figure 14-13](#), allows a user with the required privileges to edit object group-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > Object Groups**.
 - Step 2** Check the check box for the row of the object group you want to edit.
 - Step 3** Click the **Edit** button and a window appears as shown in the Object Groups window, with the object group chosen specified in the **Name** field.
 - Step 4** Enter the desired information for the object group, as specified in [Step 3](#) of the “Create” section on [page 14-21](#).
 - Step 5** Click **Save**.

The Object Groups window reappears with the edited object groups listed.

Delete

The **Delete** button, located at the bottom of the Object Groups window, allows a user with the required privileges to delete object group-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > Object Groups**.
- Step 2** Check the check box(es) for the row(s) of the object group(s) you want to delete.
- Step 3** Click the **Delete** button and a confirmation appears.
- Step 4** Click **Delete** to continue with the process of deleting information for the specified object group(s).
- The Object Groups window reappears. If this was successful, the newly updated information appears and a Status box appears in the lower left corner of the window with a green check mark for **Succeeded**.
- Otherwise click **Cancel**.
-

User Roles Design Example

This section gives an example situation, an illustration that shows this setup, and steps on how to setup this design:

- [Example, page 14-23](#)
- [Illustration of Setup, page 14-24](#)
- [Steps to Set Up Example, page 14-25](#)

Example

This section explains an example data center for which the following sections, [“Illustration of Setup” section on page 14-24](#) and [“Steps to Set Up Example” section on page 14-25](#) give an illustration setup and steps, respectively.

Finance Customer XYZ built an MPLS network to connect its branch offices to its data center. Subsidiaries of XYZ are running different parts of the MPLS network. Each subsidiary uses a different BGP AS domain, which results in different Provider Administrative Domains (PADs) inside Prime Fulfillment.

Each subsidiary acts as a Provider and owns therefore its own Devices, like PE and CE devices, and should also own logical attributes inside Prime Fulfillment, like Regions, Sites, Customers, and VPNs. Therefore, the view of the devices for each subsidiary must be separated into PAD views. Thus, Provider A cannot manipulate or view the configuration files for devices of Provider B. Devices are not shared between PADs.

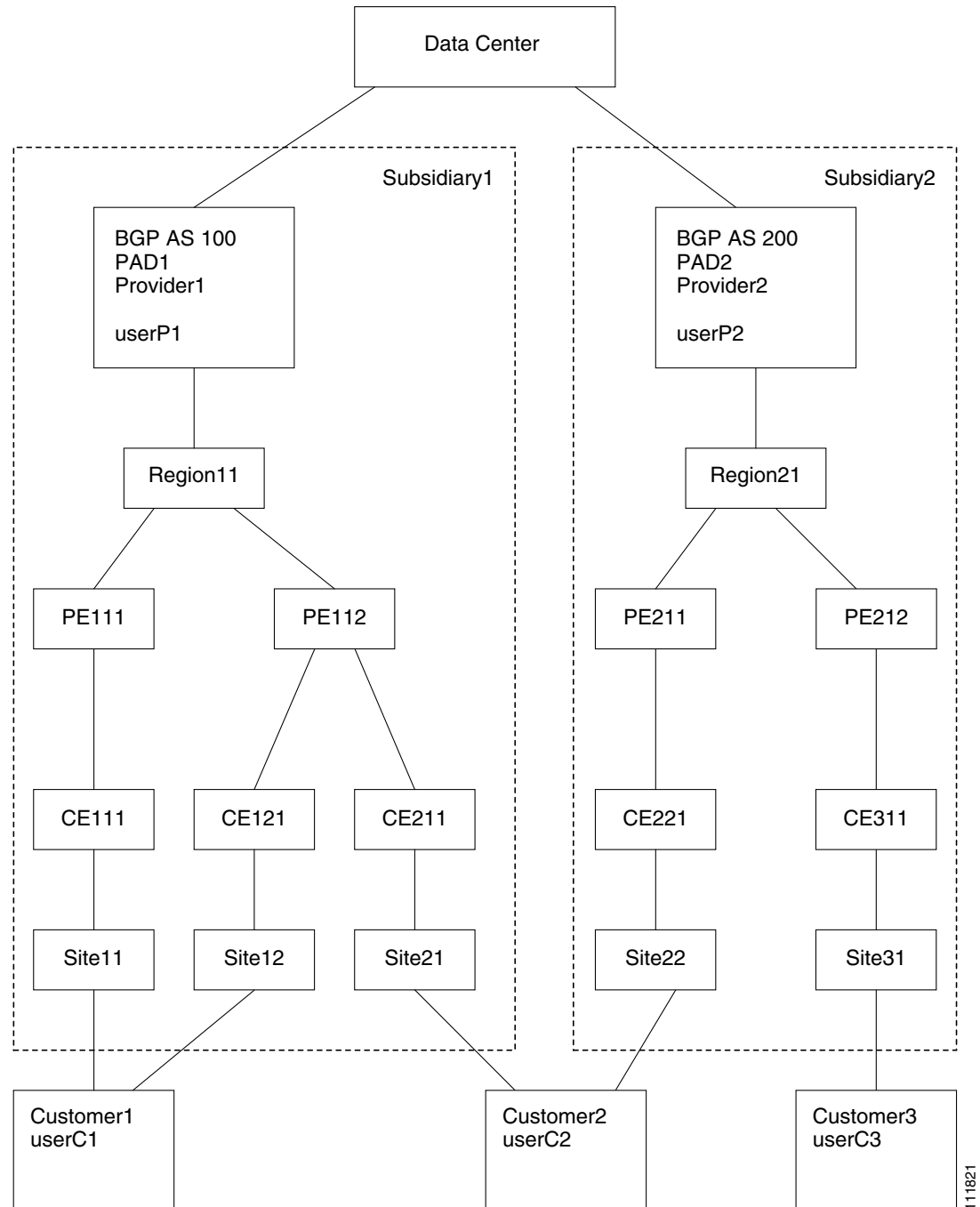
Inside a PAD, there are Customers with sites and VPNs with only local significance. Also, the IP addressing should be defined per PAD.

But there are also Customers that have sites in different PADs. This means that there is a need for Inter-AS VPNs. The Provider who owns the Customer should also have the right to share this Customer with other Providers. In this case, the VPNs and Route Targets should be shared between the providers.

Illustration of Setup

Figure 14-14 shows the setup described in the “Example” section on page 14-23.

Figure 14-14 Contents in Example



111821

Steps to Set Up Example

This section explains the steps to create the example explained in the “[Example](#)” section on page 14-23 and shown in the “[Illustration of Setup](#)” section on page 14-24.

-
- Step 1** Create the following Object Groups (see the “[Create](#)” section on page 14-21, which is for the section [Object Groups](#)):
- P1PEGroup that has members PE111 and PE112
 - P2PEGroup that has members PE211 and PE212
 - C1CEGroup that has members CE111 and CE121
 - C2CEGroup that has members CE211 and CE221
 - C3CEGroup that has the member CE311
 - C2DeviceGroup that has members PE112, CE211, PE211, and CE221
 - C3DeviceGroup that has members PE212 and CE311.
- Step 2** Create the following User Roles that are associated with one or more groups created in [Step 1](#) (see the “[Create](#)” section on page 14-17, which is for the section [User Roles](#)).
- P1DeviceGroupRole, associated with groups P1PEGroup, C1CEGroup, and C2CEGroup, and have the Modify and Delete permissions on for PE and Cpe.
 - P2DeviceGroupRole, associated with groups P2PEGroup, C2CEGroup, and C3CEGroup, and have the Modify and Delete permissions on for PE and Cpe.
 - C1DeviceGroupRole, associated with groups P1PEGroup, C1CEGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.
 - C2DeviceGroupRole, associated with group C2DeviceGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.
 - C3DeviceGroupRole, associated with group C3DeviceGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.
- Step 3** Create the following User Roles that have Customer View or Provider View, as explained in the “[User Roles](#)” section on page 14-16.
- P1MplsRole, associated with Provider P1, and have permissions on Provider, Task, Prime Fulfillment Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
 - P2MplsRole, associated with Provider P2, and have permissions on Provider, Task, Prime Fulfillment Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
 - C1MplsRole, associated with Customer C1, and have permissions on Customer, Task, Prime Fulfillment Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
 - C2MplsRole, associated with Customer C2, and have permissions on Customer, Task, Prime Fulfillment Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
 - C3MplsRole, associated with Customer C3, and have permissions on Customer, Task, Prime Fulfillment Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)

Step 4 Assign the User Roles defined in [Step 2](#) and [Step 3](#) to Users, as explained in the “Users” section on [page 14-9](#).

- User P1 has User Roles: P1DeviceGroupRole, P1MplsRole, C1MplsRole, and C2MplsRole.
- User P2 has User Roles: P2DeviceGroupRole, P2MplsRole, C2MplsRole, and C3MplsRole.
- User C1 has User Roles: C1DeviceGroupRole and C1MplsRole.
- User C2 has User Roles: C2DeviceGroupRole and C2MplsRole.
- User C3 has User Roles: C3DeviceGroupRole and C3MplsRole.

User Access Log

This section shows a detailed report of every activity by every user.

Choose **Administration > User Access Log > User Access Log** and follow these steps:

Step 1 After you choose **Administration > User Access Log > User Access Log**, a window appears as shown in [Figure 14-15](#).

Figure 14-15 User Access Log Viewer with Simple Filter



The screenshot shows the 'User Access Log' viewer. At the top, there are radio buttons for 'Simple Filter' (selected) and 'Advanced Filter', along with a 'Find' button. Below this is a 'Filter By' dropdown set to 'Date' and a 'Matches' input field containing an asterisk (*). A status bar indicates 'Showing 1 - 10 of 21,865 records'. The main table has the following columns: #, Date, Time, User Name, Origin Host, Action, Object, Severity, Activity, and Message. The table displays 10 rows of log entries, mostly showing successful logins for 'backendadm' and 'admin' users. At the bottom, there is a 'Rows per page' dropdown set to 10 and pagination controls showing 'Page 1 of 2187'.

#	Date	Time	User Name	Origin Host	Action	Object	Severity	Activity	Message
1	2011/11/18	06:15:46	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
2	2011/11/18	06:15:46	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
3	2011/11/18	06:15:46	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
4	2011/11/18	06:12:09	admin	10.65.201.96	Logon	User	INFO	SecurityActivity	Login successfully.
5	2011/11/18	06:12:04	admin	10.65.201.96	Logoff	User	INFO	SecurityActivity	Logoff.
6	2011/11/18	06:11:35	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
7	2011/11/18	06:11:35	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
8	2011/11/18	06:11:35	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
9	2011/11/18	06:10:34	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
10	2011/11/18	06:10:34	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.

All the log information about user actions appears.



Note

The types of activities or objects to be logged can be configured. This can be done directly through SQL. By default, security-related activities and activities on objects listed in the Role editor are logged.

Step 2 The default **Simple Filter** radio button is selected. To filter using the **Simple Filter**, continue with [Step 3](#). To filter using **Advanced Filter**, proceed to [Step 5](#).

Step 3 To filter the information with **Simple Filter**, keep the **Simple Filter** radio button selected and from **Filter By**, choose: **Date**, **User Name**, **Origin Host**, **Action**, **Severity**, or **Activity** (also column names). For **Matches**, enter the beginning characters of what you want to match followed by *. Then click **Find**. The result is that only the log information matching the entered filter appears.

Step 4 To exit this log report, choose another feature from the main product tabs.

Step 5 To filter the information with **Advanced Filter**, click the **Advanced Filter** radio button.

A window as shown in [Figure 14-16](#) appears.

Figure 14-16 User Access Log Viewer with Advanced Filter

User Access Log

Simple Filter **Advanced Filter** Find

Date: * Action: *
 User Name: * Severity: *
 Device Host Name: * Activity: *
 Service Requests

Showing 1 - 10 of 21,865 records

#	Date	Time	User Name	Origin Host	Action	Object	Severity	Activity	Message
1	2011/11/18	06:15:46	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
2	2011/11/18	06:15:46	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
3	2011/11/18	06:15:46	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
4	2011/11/18	06:12:09	admin	10.65.201.96	Logon	User	INFO	SecurityActivity	Login successfully.
5	2011/11/18	06:12:04	admin	10.65.201.96	Logoff	User	INFO	SecurityActivity	Logoff.
6	2011/11/18	06:11:35	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
7	2011/11/18	06:11:35	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
8	2011/11/18	06:11:35	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
9	2011/11/18	06:10:34	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
10	2011/11/18	06:10:34	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.

Rows per page: 10 Page 1 of 2187

All the log information about user actions appears.

Step 6

Enter filter information you want to match in one or more of the following categories and then click **Find**.



Note

When you choose multiple filters, the log results that appear are only the ones that match all the specified filter information.

- **Date** Enter the beginning characters of the date you want to view followed by a *, in the format given in the **Date** column.
- **User Name** Enter the beginning characters of the specific **User Name** you want to view followed by a *.
- **Device Host Name** Enter the beginning characters of the specific **Host Name** you want to view followed by a *.
- **Action** Click the drop-down list and choose from: **UNKNOWN**; **View**; **Create**; **Modify**; **Delete**; **Logon**; **Logoff**; **Session Timeout**. If you decide not to use this filter, just keep *.
- **Severity** Click the drop-down list and choose from: **UNKNOWN**; **INFO**; **WARNING**; **ERROR**. If you decide not to use this filter, just keep *.
- **Activity** Click the drop-down list and choose from: **UNKNOWN**; **SecurityActivity**; or **UserActivity**. The result is that only the log information matching the entered filter appears.

Step 7

Service Requests has a selection of **Select/Deselect**. Click this and you receive a list of Service Requests in the system from which you can check check box(es) for the User Access Log to handle. Then click the **Select** button. These Service Requests then appear on [Figure 14-16](#).

Step 8

To exit this log report, choose another feature from the main product tabs.

238504

