Cisco Prime Provisioning 6.3 Administration Guide

August 28, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27135-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Prime Provisioning 6.3 Administration Guide

CONTENTS

About This Guide

This preface contains the following sections:

Objective

The *Cisco Prime Provisioning 6.3 Administration Guide* contains detailed explanations of Cisco Prime Provisioning services and components across all applications.

Note With this release, Prime Provisioning can be used as a standalone product or as part of the Cisco Prime for IP Next Generation Network (IP NGN) Suite. When installed as part of the suite, you can launch Prime Provisioning from the Prime Central portal. For more information about Prime Central, see the documentation for Cisco Prime Central 1.1.

Audience

This guide is designed for administrators who are responsible for provisioning Prime Provisioning services for their customers.

Organization

This guide is organized as follows:

- Chapter 1, "Manage Active Users and User Account," explains how to communicate with active users and manage the user account.
- Chapter 2, "Manage Control Center," describes how to set up the Prime Provisioning services.
- Chapter 3, "Manage Security" describes how to create users, user groups, user roles, and object groups and how privileges are assigned to these entities.
- Chapter 4, "WatchDog Commands" provide supplementary information.

Related Documentation

The entire documentation set for Prime Provisioning, can be accessed at:

http://www.cisco.com/en/US/products/ps12199/tsd_products_support_series_home.html

or at:

http://www. cisco.com/go/provisioning

The following documents comprise the Prime Provisioning 6.3 documentation set:

General Documentation (in suggested reading order)

- *Cisco Prime Provisioning 6.3 Documentation Overview*
- *Cisco Prime Provisioning 6.3 Release Notes*
- *Cisco Prime Provisioning 6.3 Installation Guide*
- *Cisco Prime Provisioning 6.3 Supported Devices*
- *Cisco Prime Provisioning 6.3 User Guide*
- *Cisco Prime Provisioning 6.3 Open Source*

API Documentation

- *Cisco Prime Provisioning 6.3 API Programmer Guide*
- *Cisco Prime Provisioning 6.3 API Programmer Reference*

Note All documentation *might* be upgraded over time. All upgraded documentation will be available at the same URLs specified in this document.

Other Cisco Prime Product Documentation

See also the documentation for the following Cisco Prime products:

- *Cisco Prime Central 1.1*
- *Cisco Prime Network 3.9*
- *Cisco Prime Optical 9.6*
- *Cisco Prime Performance Manager 1.2*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Manage Active Users and User Account

This chapter explains how to communicate with active users and manage the user in Cisco Prime Provisioning.

This chapter contains the following sections:

- Active Users, page 1-1
- User Account, page 1-1

Active Users

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

Step 1 After you choose **Administration> Active Users > Active Users**, an 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 all the 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**.

CHAPTER 2

Manage Control Center

This chapter 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.

This chapter contains the following sections:

- Hosts, page 2-1
- Licensing, page 2-5
- Reporting Mechanism, page 2-6

Hosts

Hosts allows you to manage the various servers. To access 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 2-1—Available only when the host system is chosen.
- Config, page 2-2—Available only when the host system is chosen.
- Servers, page 2-3—Available only when the host system is chosen.
- Watchdog, page 2-4—Available only when the host system is chosen.
- Logs, page 2-5—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.

. The Host Details window appears. This shows the details about the chosen host.

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

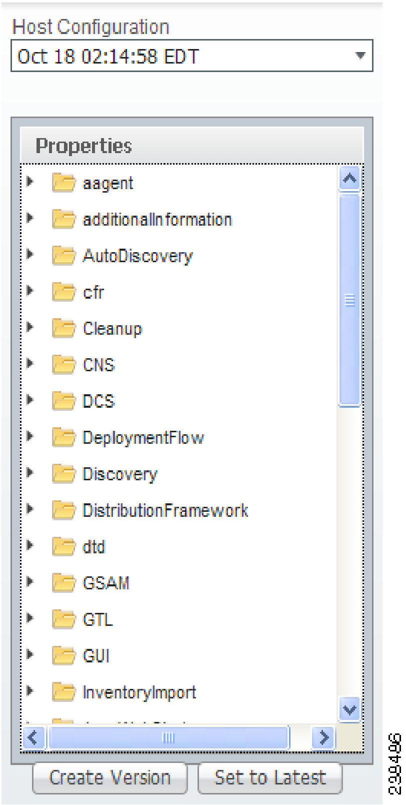
Config

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 2-1, appears. It is a list of all the folders with all the properties. Select each property to view the explanations, defaults, and ranges/rules. If you do not know the property name, you can use a key word and do a Find.

Figure 2-1 Properties



Host Configuration
Oct 18 02:14:58 EDT

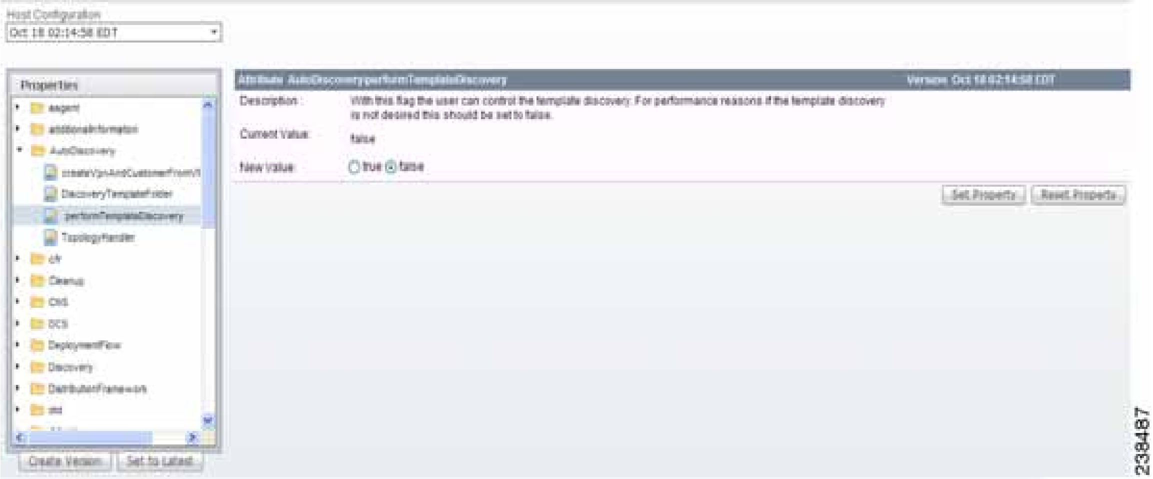
Properties
- aagent
- additionalInformation
- AutoDiscovery
- cfr
- Cleanup
- CNS
- DCS
- DeploymentFlow
- Discovery
- DistributionFramework
- dtd
- GSAM
- GTL
- GUI
- InventoryImport

Step 2 Click the arrow to expand each folder.

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

Step 3 Click on an entry to get details and instructions on how to change the value, as shown in the example in Figure 2-2.

Figure 2-2 Properties Detail Example



Attribute: AutoDiscovery.performTemplateDiscovery Version: Oct 18 02:14:58 EDT

Description : With this flag the user can control the template discovery. For performance reasons if the template discovery is not desired this should be set to false.

Current Value: false

New Value: ○ true ● false

Step 4 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 5 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 6 To view the values of previous versions of property sets, click the drop-down list on top of the window and select any version you choose.

Step 7 When you click **Set to Latest** after selecting a version in Step 6, this version is dated as the most current.

Step 8 To return, click to the navigation path you want to use next.

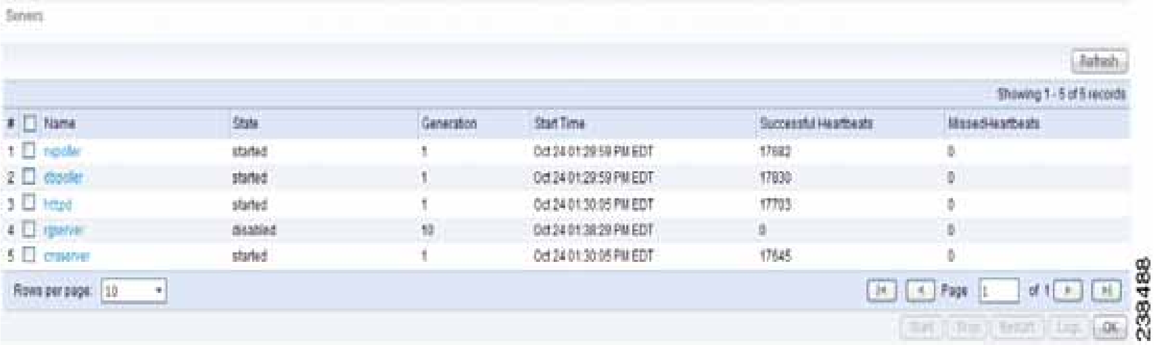
Servers

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 2-3, appears.

Figure 2-3 Servers



Servers

Showing 1 - 5 of 5 records

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

Rows per page: 10

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 2-3.

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 2-3, you return to the Control Center Hosts window.

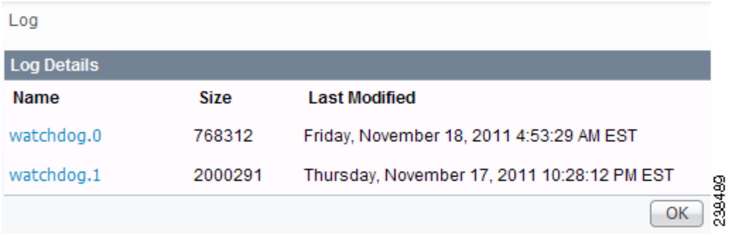
Watchdog

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 2-4, "WatchDog Logs," appears.

Figure 2-4 WatchDog Logs



Log

Log Details

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

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 2-4.

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

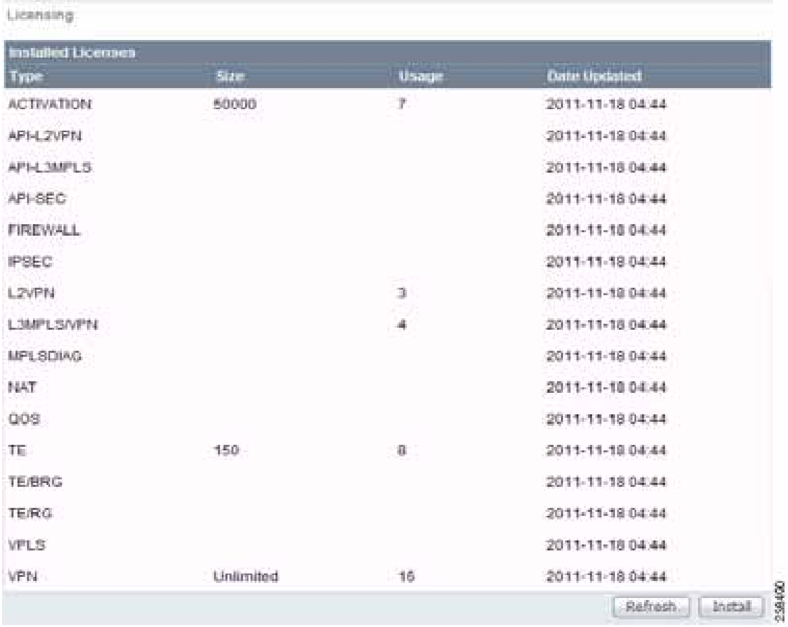
Licensing is where you install license keys, which is the only way to access services and APIs. The full version license key that is delivered, provides unlimited activation and unlimited VPNs and optional set of TEM activation license keys separately. To access Licensing:

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 2-5, appears.

Figure 2-5 Choose Administration > Control Center > Licensing



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 2-5. 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 a full version license key all features except TE, TE/BRG, TE/RG are activated with unlimited activation and unlimited VPNs.

Note The TE licenses can be purchased separately based on the number of nodes/devices available in the inventory. The total number of devices and corresponding device type, IOS/XR version, and platform info is reported by utilizing the reporting mechanism available with the product. Refer Reporting Mechanism, page 2-6 for the details of executing a reporting mechanism. 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 Provisioning 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

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 o f the Installed License table, as shown in Figure 2-5.

Step 5 Repeat Step 2, Step 3, and Step 4 for each of the *Right to Use* documents shipped with your product.

Note Upgrade licenses are only available for TE and when you receive multiple Right to Use documents to upgrade TE, be sure to enter the licenses in correct order. For example if you are upgrading from 100 to 200 TE node counts there are two step to upgrade, enter the license to upgrade to 100 to 150 and then enter license key to upgrade from 150 to 200

Reporting Mechanism

Reporting mechanism is a tool used to export the devices available in the inventory. The report includes device name, device type, platform, and IOS/IOS XR version.

To execute the reporting tool:

Step 1 Source the environment from provisioning home directory.

./prime.sh shell

Step 2 Make sure, necessary execute permissions are available for the following files:

```
<PRIMEF _HOME>/resources/nbi/scripts/getDevices
<PRIMEF _HOME>/resources/nbi/scripts/queries/DevicesQuery
<PRIMEF _HOME>/resources/nbi/scripts/util/Login
<PRIMEF _HOME>/resources/nbi/scripts/util/checkForErrors
```

Step 3 Execute the following script from <PRIMEF_HOME>/resources/nbi/scripts

./getDevices

Step 4 The resulting report can be found in <PRIMEF _HOME>/resources/nbi/scripts/Devices_Info.csv.

CHAPTER 3

Manage Security

This chapter describes how you can 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 Provisioning 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.

This chapter contains the following sections:

- Users, page 3-1—To manage users.
- User Groups, page 3-5—To manage user groups.
- User Roles, page 3-7—To manage user roles.
- Object Groups, page 3-12—To manage object groups.
- User Roles Design Example, page 3-14—Shows example of how to use the Users, User Groups, User Roles, and Object Groups

Users

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

The explanations of the buttons are given as follows:

- Details, page 3-2—View a User Detail Report
- Create, page 3-2—Create a new user
- Copy, page 3-4—Make a copy of an existing user and make changes to create a new user
- Edit, page 3-4—Edit selected user
- Delete, page 3-5—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.

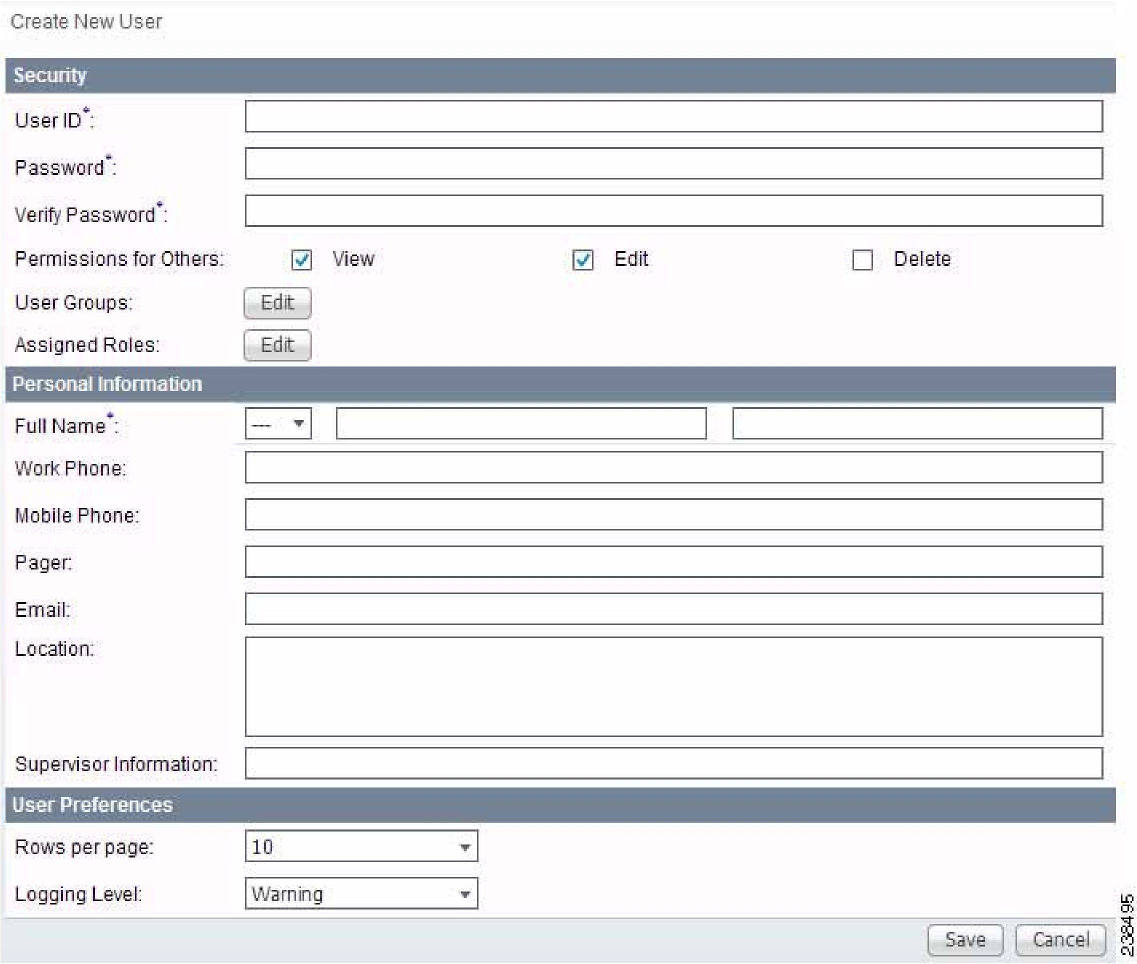
Create

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 3-1, appears.

Figure 3-1 Create/Copy/Edit Users Window



Create New User

Security

User ID*:

Password*:

Verify Password*:

Permissions for Others: ☑ View ☑ Edit □ Delete

User Groups: Edit

Assigned Roles: Edit

Personal Information

Full Name*: ---

Work Phone:

Mobile Phone:

Pager:

Email:

Location:

Supervisor Information:

User Preferences

Rows per page: 10

Logging Level: Warning

Save Cancel

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 Provisioning requires a non-blank password.
  - Prime Provisioning passwords must be a minimum of five characters and no practical maximum length.
  - Prime Provisioning does not employ any password restrictions or complexity rules; use good judgment in determining passwords.
  - Prime Provisioning passwords are encrypted when stored in the repository.
  - Prime Provisioning passwords do not expire.
  - Prime Provisioning monitors inactivity and auto-logoff per the settings defined in the Dynamic Component Properties Library (DCPL) properties for **repository/rbac.**
- **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**.
- **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 3-6).
- **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 3-1, 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 3-2.

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 3-1, 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 2**.

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 3-5—Create a new user group
- Edit, page 3-6—Edit selected user group
- Delete, page 3-7—Delete selected user group(s)

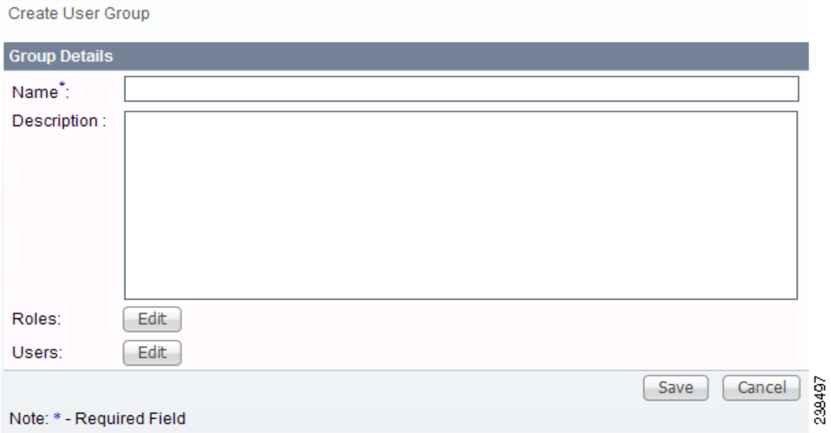
Create

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 3-2, appears.

Figure 3-2 Create/Edit User Groups Window



Create User Group

Group Details

Name*:

Description :

Roles: Edit

Users: Edit

Save Cancel

Note: * - Required Field

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 3-2, appears.

Step 4 Enter the desired information for the user group profile, as specified in Step 3 of the **"Create" section on page 3-5**.

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 Provisioning 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 3-8—Create a new user role
- Copy, page 3-11—Copy selected user role
- Edit, page 3-11—Edit selected user role
- Delete, page 3-11—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 3-3 and Figure 3-4, appears.

Figure 3-3 Create/Copy/Edit User Roles Window (Top)

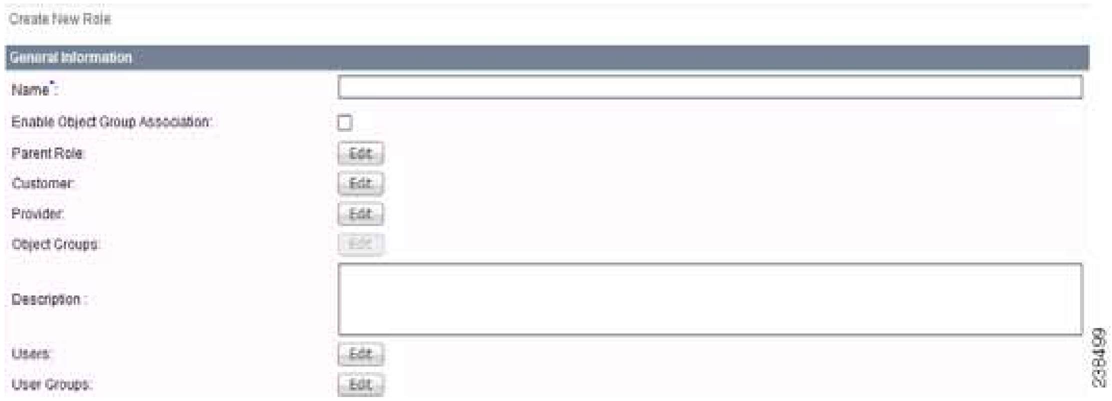
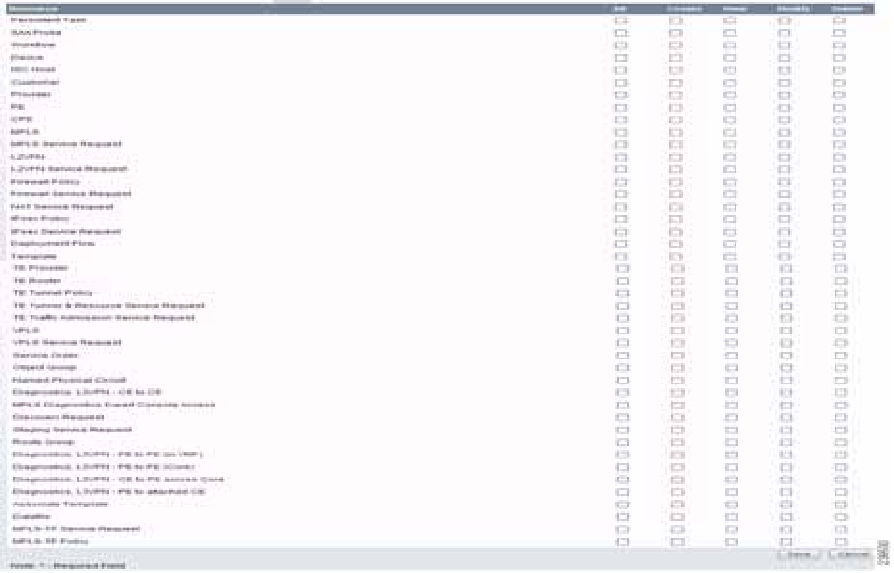


Figure 3-4 Create/Copy/Edit User Roles Window (Bottom)



Step 3 Enter the following information in Figure 3-3:

- **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 3-4, 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 is 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 3-4, click any combination of the following permissions: **Create**; **View**; **Modify**; **Delete**. If you want all the permissions, click **All**.

Note **Prime Provisioning 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 Provisioning 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 3-3 and Figure 3-4 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 3-8.

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 3-3 and Figure 3-4 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 3-8.

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 3-14.

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 3-8—Create a new object group
- Edit, page 3-11—Edit a selected object group
- Delete, page 3-11—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 **Create Object Group** window appears.

Step 3 Enter the following information:

- **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**. When you return to **Create Object Group** window, 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 **Create Object Group** window 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 **Create Object Group** window and the **Name** for each NPC Group Member appears.

Step 4 Click **Save**.

Create Object Group window reappears with the new object group listed.

Edit

The **Edit** button, located at the bottom of **Create Object Group** window, 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 3-12.

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 3-14
- Illustration of Setup, page 3-15
- Steps to Set Up Example, page 3-16

Example

This section explains an example data center for which the following sections, "Illustration of Setup" section on page 3-15 and "Steps to Set Up Example" section on page 3-16 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 Provisioning.

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 Provisioning, 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.

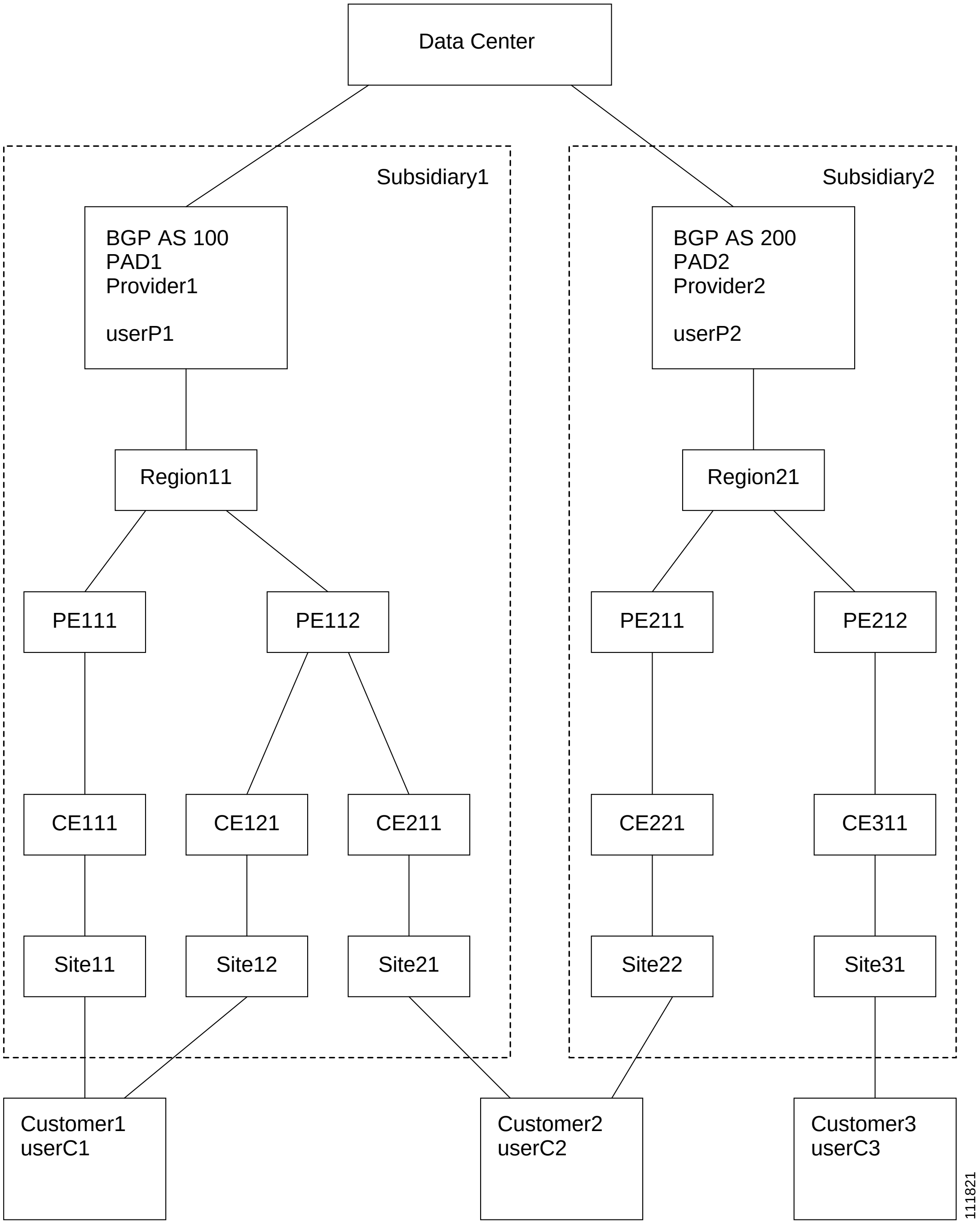
Inside a PAD, there are Customers with sites and VPNs with only local significance. Also, the IP addressing should be defined per PAD.

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 3-5 shows the setup described in the "Example" section on page 3-14.

Figure 3-5 Contents in Example



Steps to Set Up Example

This section explains the steps to create the example explained in the "Example" section on page 3-14 and shown in the "Illustration of Setup" section on page 3-15.

Step 1 Create the following Object Groups (see the "Create" section on page 3-12, 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 3-8, 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 3-7.

- P1MplsRole, associated with Provider P1, and have permissions on Provider, Task, Prime Provisioning 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 Provisioning 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 Provisioning 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 Provisioning 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 Provisioning 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 3-1.

- 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.

CHAPTER 4

WatchDog Commands

The WatchDog is responsible for bootstrapping Prime Provisioning and starting the necessary set of server processes. In addition, the WatchDog monitors the health and performance of each server to ensure it is functioning properly. In the event of a software error that causes a server to fail, the WatchDog automatically restarts the errant server.

The WatchDog is a background daemon process that is automatically installed as part of the installation procedure for Prime Provisioning. After the installation procedure has completed, WatchDog is started automatically. You can execute the **startwd** command to run the WatchDog after the installation. The WatchDog can be configured to automatically start any time the machine is rebooted.

In addition to the commands that are specified in this chapter, in the product you can choose **Administration** > **Control Center** > **Hosts** and from there you can start, stop, restart, and view log files for the individual Prime Provisioning servers.

This chapter provides the description, syntax, and arguments (listed alphabetically) for the following WatchDog commands:

startdb Command

This section provides the description and syntax for the **startdb** command.

Description

The **startdb** command starts the database.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh startdb

The **startdb** command has no arguments and starts the database.

The location of **startdb** is: *<Prime Provisioning Directory>*/**bin**.

Note Do *not* run **startdb** in the background. Do *not* enter **startdb &**.

startns Command

This section provides the description and syntax for the **startns** command.

Description

The **startns** command starts the name server. The **orbd** process provides the name server functionality. **orbd** (from JDK) is required, but **startwd** starts it if it is not already running. The **startns** and **stopns** commands deal with **orbd**.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh startns

The **startns** command has no arguments and starts the name server.

The location of **startns** is: *<Prime Provisioning Directory>*/**bin**.

startwd Command

This section provides the description and syntax for the **startwd** command.

Description

The **startwd** command starts the WatchDog and all Prime Provisioning processes. The **startwd** command includes the functionality of **startdb** (see the "startdb Command" section on page 4-1) and **startns** (see the "startns Command" section on page 4-2). Executing this command is a necessary procedure and occurs automatically as part of the installation. Use this **startwd** command after issuing a **stopwd** command to restart the WatchDog.

If for some reason the Prime Provisioning host is stopped, either inadvertently or by issuing the **stopwd** command, it can be restarted by using the **startwd** command.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh startwd

The **startwd** command has no arguments and starts the WatchDog only for the machine where it is executed.

The location of **startwd** is: <*Prime Provisioning Directory*>**/bin**

Note Do *not* run **startwd** in the background. Do *not* enter **startwd &**.

stopall Command

This section provides the description and syntax for the **stopall** command.

Description

The **stopall** command stops the database, name server, and WatchDog on the machine on which it is run. The **stopall** command includes the functionality of **stopdb -y** (see the "stopdb Command" section on page 4-3), **stopns -y** (see the "stopns Command" section on page 4-4), and **stopwd -y** (see the "stopwd Command" section on page 4-4). Normally this is only necessary before installing a new version of Prime Provisioning.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh stopall

Caution There is no **-y** parameter. Therefore, everything stops without the ability to cancel.

The location of **stopall** is: <*Prime Provisioning Directory*>**/bin**.

stopdb Command

This section provides the description and syntax for the **stopdb** command.

Description

The **stopdb** command stops the database.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh stopdb [**-y**]

where:

-y indicates not to prompt before shutdown. If **-y** is not specified, you are prompted with the following message: "Are you absolutely sure you want to stop the database?" You are then prompted to reply **yes** or **no**.

The location of **stopdb** is: <*Prime Provisioning Directory*>/**bin**.

stopns Command

This section provides the description and syntax for the **stopns** command.

Description

The **stopns** command stops the name server. The **startns** and **stopns** commands deal with **orbd**.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh stopns [**-y**]

where:

-y indicates not to prompt before shutdown. If **-y** is not specified, you are prompted with the following message: "Are you absolutely sure you want to stop the nameserver?" You are then prompted to reply **yes** or **no**.

The location of **stopns** is: <*Prime Provisioning Directory*>/**bin.**

stopwd Command

This section provides the description and syntax for the **stopwd** command.

Description

The **stopwd** command stops the WatchDog and all Prime Provisioning processes other than the name server and the database.

Syntax

Go to **PRIMEP_HOME** and execute the following command:

./prime.sh stopwd [**-y**]

where:

-y indicates not to prompt before shutdown. If **-y** is not specified, you are prompted with the following message: "Are you absolutely sure you want to stop the watchdog and all of its servers? Other users may be using this system as well. No activity (for example: collections, performance monitoring, provisioning) occurs until the system is restarted." You are then prompted to reply **yes** or **no**.

The location of **stopwd** is: <*Prime Provisioning Directory*>**/bin**.

wdclient Command

This section provides the description, syntax, and options (listed alphabetically) for the **wdclient** subcommands. These subcommands are diagnostic tools. This section also describes the column format of the output of each of the subcommands.

Note The location of **wdclient** is: <*Prime Provisioning Directory*>**/bin**.

The following are the **wdclient** subcommands:

- wdclient disk Subcommand, page 4-5
- wdclient group <group_name> Subcommand, page 4-6
- wdclient groups Subcommand, page 4-6
- wdclient health Subcommand, page 4-6
- wdclient restart Subcommand, page 4-7
- wdclient start Subcommand, page 4-7
- wdclient status Subcommand, page 4-8
  - Information Produced: Name Column, page 4-8
  - Information Produced: State Column, page 4-9
  - Information Produced: Gen Column, page 4-9
  - Information Produced: Exec Time Column, page 4-9
  - Information Produced: Success Column, page 4-9
  - Information Produced: Missed Column, page 4-9
- wdclient stop Subcommand, page 4-10

Note If you enter **wdclient -help**, you receive a listing of all the wdclient subcommands.

wdclient disk Subcommand

This section provides the description and syntax for the **wdclient disk** subcommand.

Description

The **wdclient disk** subcommand gives the disk space statistics for the directories where Prime Provisioning is installed.

Syntax

wdclient disk

wdclient group <*group_name*> Subcommand

This section provides the description and syntax for the **wdclient group <*group_name*>** subcommand.

Description

The **wdclient group <*group_name*>** subcommand lists the servers in the specified server group. Server groups provide a convenient way to start or stop a group of servers with a single command.

Syntax

wdclient group <*group_name*>

where:

<*group_name*> is the name of a server group chosen from the list displayed by the **wdclient groups** command.

wdclient groups Subcommand

This section provides the description and syntax for the **wdclient groups** subcommand.

Description

The **wdclient groups** subcommand lists all the active server groups.

Syntax

wdclient groups

wdclient health Subcommand

This section provides the description and syntax for the **wdclient health** subcommand.

Description

The **wdclient health** subcommand indicates whether all the servers are stable.

Syntax

wdclient health

wdclient restart Subcommand

This section provides the description and syntax for the **wdclient restart** subcommand.

Description

The **wdclient restart** subcommand restarts one or more servers. Any dependent servers are also restarted.

Note It is not necessary to restart servers in a properly functioning system. The **wdclient restart** command should only be run under the direction of Cisco Support.

Syntax

wdclient restart [**all** | <*server_name*> | **group** <*group_name*>]

where you can choose one of the following arguments:

all is all servers. This is the default if no argument is specified.

<*server_name*> is the name of a server chosen from the list displayed by the **wdclient status** command. See Table 4-1, "Servers and Their Functions," for server descriptions.

group <*group_name*> where, <*group_name*> is the name of a server group chosen from the list displayed by the **wdclient groups** command.

wdclient start Subcommand

This section provides the description and syntax for the **wdclient start** subcommand.

Description

The **wdclient start** subcommand starts one or more servers. Other servers that depend on the specified server(s) might also start.

Note It is not necessary to stop and start servers in a properly functioning system. The **wdclient start** command should only be run under the direction of Cisco Support.

Syntax

wdclient start [**all** | <*server_name*> | **group** <*group_name*>]

where you can choose one of the following arguments:

all is all servers. This is the default if no argument is specified.

<server_name> is the name of a server chosen from the list displayed by the **wdclient status** command. See Table 4-1, "Servers and Their Functions," for server descriptions.

group *<group_name>* where, *<group_name>* is the name of a server group chosen from the list displayed by the **wdclient groups** command.

wdclient status Subcommand

This section provides the description, syntax, and information produced for the **wdclient status** subcommand.

Description

The **wdclient status** subcommand lists all the servers and their states. See Table 4-1 on page 4-8, "Servers and Their Functions," for server descriptions. See Table 4-2 on page 4-9, "Valid States," for the list of all the states.

Syntax

wdclient [**-poll** *<seconds>*] **status**

where:

-poll *<seconds>* is an optional parameter. *<seconds>* is the number of seconds. A number other than zero indicates that when new status data is available it is displayed every *<seconds>* seconds, where *<seconds>* is the specified number of seconds. The default **-poll** value is zero (0), which shows the status just once.

Information Produced: Name Column

The **Name** column provides the name of each of the servers. Table 4-1 provides a list of the servers and a description of the function that each server provides.

Table 4-1 Servers and Their Functions

Server	Function
cnsserver	Handles TIBCO messages from Cisco Configuration Engine servers and takes appropriate actions.
dbpoller	Monitors database server.
discovery	Devices and Service Discovery Engine.
httpd	Web server.
nspoller	Monitors name service.
rgserver	Executes various Prime Provisioning traffic engineering computations, such as tunnel repairing.

Note The processes that no longer exist includes dispatcher, lockmanager, scheduler, and worker.

Information Produced: State Column

The **State** column provides the current state of the server. Table 4-2 provides a description of each of the states in normal progression order.

Table 4-2 Valid States

State	Description
start_depends	This server has been asked to start, but is waiting for servers it depends on to start. After all dependent servers have started, this server transitions to the state of starting.
starting	This server is currently starting. After a successful heartbeat occurs, this server transitions to the state of started.
started	This server is currently started and running.
stop_depends	This server is supposed to be stopped, but it is waiting for servers it depends on to be stopped first.
stopping_gently	This server is in the process of stopping in a gentle fashion. That is, it was notified that it is to stop.
stopping_hard	This server is in the process of being killed because either it did not have a way to stop gently or because the gentle stop took too long.
stopped	This server is stopped. The WatchDog either starts it again or disables it if it has been frequently dying.
disabled_dependent	This server is disabled because one or more servers it depends on are disabled. If all servers it depends on are started, this server automatically starts.
disabled	This server is disabled and must be manually restarted.
restart_delay	This server is delaying before restarting. There is a short delay after a server stops and before it is restarted again.

Information Produced: Gen Column

The **Gen** column provides the generation of the server. Each time the server is started, the generation is incremented by 1.

Information Produced: Exec Time Column

The **Exec Time** column provides the date and time the server was last started.

Information Produced: Success Column

The **Success** column provides the number of successful heartbeats since the server was last started. Heartbeats are used to verify that servers are functioning correctly.

Information Produced: Missed Column

The **Missed** column provides the number of missed heartbeats since the server was last started.

A few missed heartbeats could simply indicate the system was busy. However, more than a couple of missed heartbeats per day could indicate a problem. See the logs to diagnose the reason.

Three missed heartbeats in a row is the default for restarting the server.

wdclient stop Subcommand

This section provides the description and syntax for the **wdclient stop** subcommand.

Description

The **wdclient stop** subcommand stops one or more servers. Other servers that depend on the specified servers also stop.

Note It is not necessary to stop servers in a properly functioning system. The **wdclient stop** command should *only* be run under the direction of Cisco Support.

Syntax

wdclient stop [**all** | <*server_name*> | **group** <*group_name*>]

where you can choose one of the following arguments.

all is all servers. This is the default if no argument is specified.

<*server_name*> is the name of a server chosen from the list displayed by the **wdclient status** command. See Table 4-1, "Servers and Their Functions," for server descriptions.

group <*group_name*> is the name of a server group chosen from the list displayed by the **wdclient groups** command.