



## **Cisco Prime Central 1.5.3 User Guide**

**First Published:** 2014-02-28

### **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-28574-02

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2011–2017 Cisco Systems, Inc. All rights reserved.



## CONTENTS

?

---

### PREFACE

|  |           |
|--|-----------|
| <b>Preface</b>   | <b>xi</b> |
| Audience   | xi        |
| Related Documentation                                    | xi        |
| Obtaining Documentation and Submitting a Service Request | xii       |

---

### CHAPTER 1

|   |          |
|---|----------|
| <b>Working with the Prime Central Portal</b>  | <b>1</b> |
| Overview of the Prime Central Portal          | 1        |
| Key Features                                  | 2        |
| Security                                      | 3        |
| Logging In to the Prime Central Portal        | 4        |
| Customizing Login Advisory Messages           | 5        |
| Maximum Number of User Accounts Supported     | 7        |
| Customizing the Prime Central Portal          | 7        |
| Adding a Portlet                              | 8        |
| Maximizing or Minimizing a Portlet            | 9        |
| Removing a Portlet                            | 9        |
| Adding or Removing Columns in a Portlet       | 9        |
| Changing the Layout of the Home Page          | 10       |
| Changing the Time Zone                        | 10       |
| Changing the Prime Central Session Timeout    | 11       |
| Changing the Fault Management Session Timeout | 11       |
| Menu Structure                                | 12       |
| Home Menu                                     | 12       |
| Design Menu                                   | 12       |

|   |    |
|---|----|
| Fulfill Menu  | 13 |
| Assure Menu   | 14 |
| Analyze Menu  | 14 |
| Inventory Menu  | 15 |
| Administration Menu   | 15 |
| Filtering and Searching                                     | 16 |
| Filtering Using the Quick Filter                            | 16 |
| Filtering Using the Advanced Filter                         | 17 |
| Sorting   | 19 |
| Finding the Prime Central Version                           | 19 |
| Logging Out of the Prime Central Portal                     | 20 |
| Closing the Prime Central Browser Without Logging Out       | 20 |
| Managing the Self-Signed Certificates                       | 20 |
| Importing an Existing Certificate into WebSphere            | 20 |
| Placing Certificates in the Internet Explorer Trusted Store | 22 |

---

**CHAPTER 2**
**Managing Users and Configuring Role-Based Access Control 23**

|   |    |
|---|----|
| User Management Portlet                     | 23 |
| Managing Users                              | 24 |
| Adding a User                               | 24 |
| Name, Password, Phone, and Note Constraints | 26 |
| User Information in the Quick View          | 28 |
| Editing a User                              | 29 |
| Copying a User                              | 31 |
| Deleting a User                             | 32 |
| Resetting Another User's Password           | 32 |
| Resetting Your User Password                | 32 |
| Resetting a Lost Password                   | 33 |
| Enabling or Disabling a User Account        | 34 |
| Configuring User Security Settings          | 34 |
| Managing Groups                             | 37 |
| Adding a Group                              | 37 |
| Editing a Group                             | 37 |
| Deleting a Group                            | 38 |

|  |    |
|--|----|
| Managing Roles   | 38 |
| Adding a Role  | 41 |
| Editing a Role   | 41 |
| Deleting a Role  | 41 |
| Managing Privileges  | 42 |
| Adding a Privilege   | 43 |
| Editing a Privilege  | 44 |
| Deleting a Privilege   | 44 |
| Creating a Bulk User   | 44 |
| Importing Users in Bulk  | 44 |
| Updating Users in Bulk   | 46 |
| Retrieving Users in Bulk   | 47 |
| Deleting Users in Bulk   | 47 |
| Reporting User Logins in Bulk  | 48 |
| Exporting User Data  | 49 |
| Auditing User Activity   | 50 |
| Using an External Authentication Provider (LDAP or AAA Server) for User Authentication | 50 |
| Configuring Prime Central to Communicate with an External LDAP Server                  | 51 |
| Configuring Prime Central to Communicate with an External AAA Server                   | 53 |

---

**CHAPTER 3**
**Monitoring Prime Central and the Applications 57**

|   |    |
|---|----|
| Monitoring the Health of Prime Central and the Applications       | 57 |
| Prime Central and Application Monitoring Information              | 59 |
| Suite Monitoring Information in the Quick View                    | 60 |
| Prioritizing Application Instances                                | 60 |
| Monitoring System Activity  | 61 |
| Monitoring Prime Provisioning Service Requests                    | 64 |
| Device SR Count Portlet   | 64 |
| SR Summary Portlet  | 65 |
| Changing the Prime Central Transport Type Policy                  | 66 |
| Removing an Application Manager from the Suite Monitoring Portlet | 67 |

---

**CHAPTER 4**
**Managing Inventory 69**

|                               |    |
|-------------------------------|----|
| What Is Inventory Management? | 69 |
|-------------------------------|----|

|   |    |
|---|----|
| Common Inventory Portlet  | 69 |
| Retrieving Common Inventory Data  | 70 |
| Retrieving Common Inventory Data  | 71 |
| Common Inventory Properties Pane  | 71 |
| Synchronizing Inventory Data  | 72 |
| Retrieving Physical Inventory Data                                      | 73 |
| Regular Device Attributes for Equipment Holders and Equipment           | 74 |
| Retrieving Service Inventory Data                                       | 75 |
| Cross-Launching an Application to Retrieve Inventory Details            | 76 |
| Performing a Contextual Cross-Launch to the Data Center Hypervisor Pane | 76 |
| Device Information in the Device 360° View                              | 77 |
| Access Points Portlet   | 78 |
| Access Points Details Panel   | 79 |
| Navigating to Access Points Portlet                                     | 80 |
| Configuring Access Points   | 81 |
| Access Points Fault Management  | 84 |
| Exporting Inventory Data  | 84 |
| Grouping Network Devices and Services                                   | 85 |
| Adding a Group  | 86 |
| Editing a Group   | 87 |
| Deleting a Group  | 87 |
| Adding a Group Member   | 88 |
| Removing a Group Member   | 88 |
| Monitoring Alarm Counts for Grouped Devices                             | 88 |

---

**CHAPTER 5**
**Managing Customers 91**

|  |    |
|--|----|
| Customer Management Portlet                    | 91 |
| Managing Customers                             | 92 |
| Adding a Customer                              | 92 |
| Customer Information Constraints               | 92 |
| Customer Information in the Customer 360° View | 93 |
| Editing a Customer                             | 94 |
| Deleting a Customer                            | 95 |
| Associating Resources to Customers             | 95 |

Removing Resources from Customers 97

Exporting Customer Data 97

## CHAPTER 6

### Managing Faults 99

What Is Fault Management? 99

Fault Management Terminology 100

Alarm Processing 100

Alarm Aggregation 100

Alarm Deduplication 101

Alarm Correlation 101

Alarm Aging 102

Monitoring Affected Services and Customers 102

Opening the Alarm Browser Portlet 104

Information Displayed in the Alarm Browser Portlet 105

Accessing Additional Alarm Information 108

Viewing Alarms in the Alarm Summary 109

Acknowledging or Deacknowledging an Alarm 111

Clearing an Alarm 112

Retiring an Alarm 112

Adding Notes to an Alarm 113

Resynchronizing Applications 113

Sorting Columns 114

Refreshing Data 114

Finding Data 114

Changing the Alarm Information Displayed 115

Filtering Alarms Using the Quick Filter 115

Filtering Alarms Using the Advanced Filter 116

Creating and Editing Views 118

Freezing and Unfreezing the Alarm Browser 119

Configuring Email and SMS for Alarm Notifications 120

Changing Alarm Browser Preferences 121

Managing Prime Central Fault Sources 124

Adding a Fault Source 124

Editing a Fault Source 124

|  |     |
|--|-----|
| Deleting a Fault Source                          | 125 |
| Add New Fault Source Dialog Box                  | 125 |
| Analyzing Fault Data                             | 125 |
| Default Alarm Reports                            | 126 |
| Opening the Alarm Report Portlet                 | 127 |
| Creating a New Report                            | 129 |
| Scheduling a Report                              | 129 |
| Saving or Emailing a Report                      | 130 |
| Setting Report Properties                        | 131 |
| Specifying the Report Order                      | 131 |
| Deleting a Report                                | 132 |
| Configuring Alarms Retention Period              | 132 |
| Configuring the SNMP Gateway for NBI Integration | 133 |
| Gateway-Specific Properties                      | 133 |
| Map Definition Files                             | 136 |
| Gateways and DSAs Used with Prime Central        | 138 |

---

**CHAPTER 7**
**Monitoring Your Data Center 143**

|   |     |
|---|-----|
| Introduction  | 143 |
| Default Prime Performance Manager Reports                               | 144 |
| Overview Window   | 145 |
| Compute Window  | 147 |
| Compute Service Pane  | 147 |
| Hypervisor Pane   | 148 |
| Cluster Pane  | 149 |
| Network Window  | 149 |
| Storage Window  | 150 |
| Data Center Dashboards  | 151 |
| Data Center 360° View   | 153 |
| Synchronizing Scopes and Inventory Data                                 | 154 |
| Setting the Lifecycle State and Priority for a Compute Service Resource | 155 |
| Performing a Contextual Cross-Launch to the Common Inventory Portlet    | 156 |
| Adding Data Center Resources to Groups                                  | 156 |
| Associating Data Center Resources with Customers                        | 156 |

---

**APPENDIX A****Appendix A: Troubleshooting 157**Troubleshooting the Prime Central Integration Layer **157**Troubleshooting the Prime Central Portal **160**Troubleshooting Prime Central Security **163**Troubleshooting Prime Network **163**Troubleshooting Prime Optical **164**Troubleshooting Prime Performance Manager **166**Troubleshooting Prime Provisioning **167**Troubleshooting Prime Fault Management **168**





## Preface

---

This guide describes the structure and features of Cisco Prime Central and how to use it.

This preface contains the following sections:

- [Audience, on page xi](#)

## Audience

The primary audience for this guide is network operations personnel and system administrators. This guide assumes that you are familiar with the following products and topics:

- Basic internetworking terminology and concepts
- Network topology and protocols
- Microsoft Windows 7 and Windows XP
- Red Hat Enterprise Linux administration
- Oracle database administration
- Telecommunication Management Network (TMN) architecture model

## Related Documentation

See the [Cisco Prime Central 1.5.3 Documentation Overview](#) for a list of Prime Central guides.

See also the documentation for the following suite components:

- [Cisco Prime Network](#)
- [Cisco Prime Optical](#)
- [Cisco Prime Performance Manager](#)
- [Cisco Prime Provisioning](#)



---

**Note** We sometimes update the documentation after original publication. Therefore, you should review the documentation on Cisco.com for any updates.

---

## 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 an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.



# CHAPTER 1

## Working with the Prime Central Portal

The following topics will help you get started with the Prime Central portal:

- [Overview of the Prime Central Portal, on page 1](#)

### Overview of the Prime Central Portal

Cisco Prime Carrier Management provides end-to-end management, from access to the core, helping enable carrier-class delivery of next-generation voice, mobile, cloud, and managed services. With the modular architecture, you have the flexibility to deploy the entire integrated suite or do it incrementally as you grow your business, depending on your needs.

The Prime Central portal is the main console for operator workflows across multiple applications. The applications listed in the following table are accessible through the Prime Central portal.

**Table 1: Components of Cisco Prime Carrier Management**

| Component                     | Description   |
|-------------------------------|---|
| Prime Network                 | Provides management of packet networks, including access, aggregation, edge, MPLS core, and Evolved Packet Core (EPC).  |
| Prime Optical                 | Provides efficient and productive optical infrastructure management for fault, configuration, performance, and security.  |
| Prime Performance Manager     | Provides performance statistics and reports for service provider and large enterprise networks, including access, edge, distribution, core, mobile backhaul, Carrier Ethernet, MPLS core, and EPC networks.   |
| Prime Provisioning            | Provides automated resource management and rapid profile-based provisioning capabilities for Carrier Ethernet, Radio Access Network (RAN) backhaul, Multiprotocol Label Switching (MPLS), and Packet Transport technologies.  |
| Broadband Access Center (BAC) | It is a versatile TR-069 management system that provides all essential Femtocell management functions whether it is AP configuration, firmware, data retrieval, troubleshooting, and so on. Cisco RMS uses BAC as the TR-069 Auto Configuration Server (ACS), which contains the Regional Data Unit (RDU) and Device Provisioning Engine (DPE). |

| Component                                  | Description  |
|--|--|
| Cisco Prime Access Registrar (CPAR)        | The Prime Access Registrar (PAR) is used for AAA authentication. It provides AP authentication on the HNB-GW and delivers AP whitelists to HNB-GW via RADIUS. CPAR is an integral part of RMS solution.  |
| Cisco Prime Network Registrar (CPNR)       | The Prime Network Registrar (PNR), also called the DHCP server, is used to allocate IPsec addresses for SeGW via DHCP. The lease database can then be queried to discover the current IP address of an AP. CPNR is an integral part of RMS solution.   |
| Cisco RAN Management System (RMS) Solution | It provides different workflows and services to support enhanced provisioning and managing capabilities for both, 3G and LTE Femtocells. These services include provisioning and management functions such as, device configuration, status monitoring, firmware upgrade, data retrieval, and troubleshooting. |

See the [Cisco Prime Central 1.5.3 Release Notes](#) for the latest application versions that are compatible with Prime Central 1.5.3

## Key Features

The Prime Central portal plays the role of the presentation tier for the entire suite. The portal provides:

- A single point of access (single sign-on) to Prime Central and the individual applications.
- Support for Lightweight Directory Access Protocol (LDAP), TACACS+, and RADIUS authentication plugins.
- Common customer management and user management with role-based access control (RBAC).
- Security settings you can configure for all users in your network, such as:
  - Maximum login attempts
  - Maximum active user sessions
  - User inactivity period before deactivation
- Customizable login advisory messages.
- Email and SMS notifications when critical and major alarms occur.
- Bulk import of users specified in an Excel spreadsheet.
- Bulk reporting of user logins.
- Management of alarm and trap information sources in the Fault Source Management portlet.
- Database and application monitoring.
- Common physical inventory management:
  - Detailed physical inventory and Device 360° views.
  - Filter and search capabilities.
  - Seamless drill-down to individual applications.

- Support for multiple instances of Prime Network and Prime Optical.
- Support for Gigabit-capable Passive Optical Network (GPON) and Metro Ethernet Forum (MEF)-compliant devices.
- Common cross-application alarm management:
  - Aggregation, correlation, and deduplication of alarms.
  - Portlets with customized views and filters.
  - Seamless cross-launch of the source application.
  - Seamless access from alarms to common inventory.
  - Pregenerated reports for active and historical alarms.
  - SNMPv1, v2c, and v3 forwarding (OSS integration).
  - In addition to the Prime Central Fault Management GUI, the ability to perform tasks from Prime Network, Prime Optical, and Prime Performance Manager (when configured for Suite mode).
- Security audit information, which can be viewed in the Audit Log portlet.
- Synchronization of alarm information provided by Prime Central and associated Prime applications.
- Virtualization on VMware configurations.
- Red Hat Enterprise Linux (RHEL) 6.4 6.5 and 6.7 6.4 6.5 and 6.7support.
- Operational redundancy and disaster recovery:
  - You can install Prime Central and an embedded Oracle database in a local redundancy, high availability (HA) configuration that uses the Red Hat Cluster Suite (RHCS) in both Bare Metal and VMware environments.
  - You can also configure switchover and failover to mitigate the impact of a Cisco Prime application (like Prime Network) going down.



---

**Note** The HA and switchover/failover options must be purchased and installed separately from Prime Central 1.5.3 .

---

- Cross-launch to Cisco InTracer, a high-performance, subscriber troubleshooting and monitoring solution.
- Cross-launch to the Cisco ME 4600 Series Agora-NG network provisioning platform.
- Northbound interfaces supports MTOSI and 3GPP APIs.

## Security

Prime Central security features include:

- HTTPS support for transporting user credentials.
- SSL encryption of all single sign-on (SSO) traffic.

- URL-based SSL traffic encryption available upon configuration.
- Configurable session timeout with a default value.
- Role-based, password-protected access for multiple users.
- Password enforcement policies, such as aging, minimum length, and lockouts.
- Audit trails of all user actions and all access through the web interface.
- Cleanup of session states and expiration of cookies upon session timeout.
- Cross-site scripting and SQL injection guard.
- Mutual authentication between SSO and all SSO participating applications: Prime Network, Prime Optical, Prime Performance Manager, and Prime Provisioning.



---

**Note** For HTTPS communication, only Secure Sockets Layer version 3 (SSLv3) and Transport Layer Security version 1 (TLSv1) are allowed. The highest exportable SSL ciphers for encryption communication are used.

---

## Logging In to the Prime Central Portal

Prime Central features single sign-on (SSO), meaning that when you log in to the Prime Central portal, you do not have to log in separately to each application within your domain.

Using an open-source product called Central Authentication Service (CAS), the SSO solution offers a central authoritative source that is shared by the Prime Central portal and applications.

With an SSO CAS solution, different applications can authenticate to one authoritative source of trust. You then log in to that single source; you do not have to log in to each application separately. Any authentication provider (such as RADIUS, TACACS+, or LDAP) can use the eXtensible Management Platform (XMP) login mechanism within the CAS authentication handler. CAS SSO applies to all web applications that are running under the same browser session.

### Procedure

---

- Step 1** Open a Prime Central-supported web browser and enter **https://server-hostname:https-port-number**, where:
- *server-hostname* is the hostname of the Prime Central portal.
  - *https-port-number* is the SSL port number that was configured during installation. The default SSL port is 8443.

- Note** Use a Prime Central-supported browser as your default web browser with caching and cookies enabled. If you log in to Prime Central with a web browser that is not your default browser:
- You might need to log in again when you cross-launch from one application to another.
  - A cross-launched application might remain open even after you log out of Prime Central.

The login window (see the following figure) opens.

**Step 2** Enter your username and password.

If you are an administrator logging in for the first time, enter the username *centraladmin* and the password that you configured during installation.

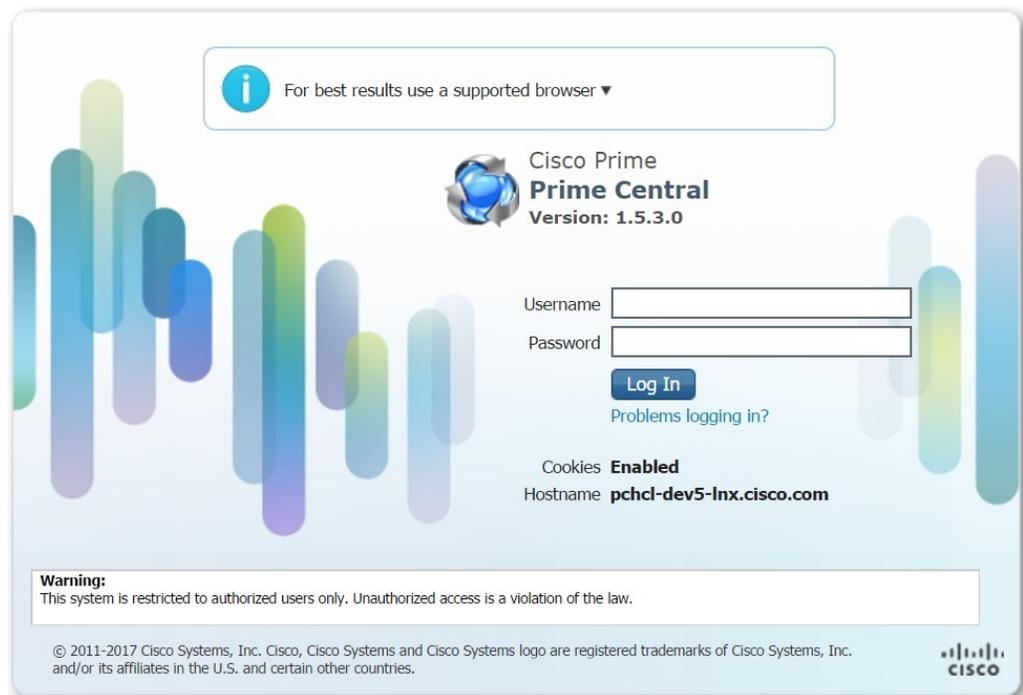
**Step 3** Click **Log In**.

**Step 4** Click **Agree**.

**Step 5** Accept the self-signed, untrusted security certificates.

- In Firefox, if you accept the security certificates, they do not reappear upon subsequent logins.
- In Internet Explorer, if you accept the security certificates without placing them in the trusted certificate store, they reappear upon subsequent logins. If you place the certificates in the trusted store, they do not reappear upon subsequent logins. See [Placing Certificates in the Internet Explorer Trusted Store](#).

**Figure 1:**



## Customizing Login Advisory Messages

Advisory messages are shown both before and after a user logs into Prime Central. By default, these messages read as follows:

- Pre-login message—Warning: This system is restricted to authorized users only. Unauthorized access is a violation of the law.
- Post-login terms-of-use message—Warning: You are accessing a private network. Unauthorized access is a violation of the law.

## Customizing the Pre-Login Advisory Message

### Procedure

- 
- Step 1** Log in to the Prime Central portal as the primeusr user.
  - Step 2** In a text editor, open the `$XMP_HOME/tomcat-7.0.23/webapps/ROOT/html/xmp/xwt/nls/en-us/sso_login.js` file.
  - Step 3** Update the `login_disclosure` variable with the desired text changes.
  - Step 4** Save your changes to the `sso_login.js` file.
  - Step 5** Restart the Prime Central portal.
  - Step 6** Log out of the Prime Central portal, clear your browser cache, and log back in.
- 

## Customizing the Terms-of-Use Message That Appears After Login

### Procedure

- 
- Step 1** Log in to the Prime Central portal as a user with administrator-level privileges.
  - Step 2** From the Prime Central menu, choose **Administration > System > Global Settings**.
  - Step 3** In the Global Settings portlet (see the following figure), modify the terms-of-use text as desired.
  - Step 4** To configure when users see the terms-of-use message, click one of the following radio buttons:
    - **Enable**—The terms-of-use message appears every time a user logs into Prime Central.
    - **Disable**—The terms-of-use message appears only the first time a user logs into Prime Central.
  - Step 5** Click **Save**.

*Figure 2: Global Settings Portlet*

The screenshot shows a web interface titled "Global Settings". Under the heading "Terms of Use", there is a text area containing the message: "Warning: You are accessing a private network. Unauthorized access is a violation of the law." Below the text area, there are two radio buttons: "Enable" (which is selected) and "Disable". At the bottom of the portlet, there are two buttons: "Save" and "Cancel".

## Maximum Number of User Accounts Supported

Prime Central supports up to 150 simultaneous users, all of whom can see their own customized view of the Prime Central portal.

Note the following:

- In Prime Central, 30 users can perform all portal operations concurrently. The remaining 120 users can monitor data, but it is not recommended that they perform memory-intensive operations such as application cross-launch or user management.
- A single user can have up to ten cross-launched application windows open simultaneously. If a user tries to open an eleventh window, the user cannot proceed without first closing one of the open windows.
- Prime Central supports up to 30 simultaneous application cross-launches across multiple users.
- The number of application cross-launches Prime Central supports depends on:
  - CPU and memory available on a user's machine.
  - CPU, memory, and connections available on the machines on which the individual applications run.

## Customizing the Prime Central Portal

When you log in to Prime Central, the portlets that you see on the home page depend on your user privileges and which applications are installed and available. The following figure shows the Prime Central home page with the Alarm Browser portlet partially visible.

Figure 3: Prime Central Home Page



|   |  |    |                           |
|---|--|----|---------------------------|
| 1 | Content area, with content that depends on your portlet selections | 9  | Refresh Current Page icon |
| 2 | Menu bar, with main menu choices                                   | 10 | Help icon                 |
| 3 | Home menu and icon   | 11 | Remove icon               |
| 4 | <i>Logged-in user</i> link   | 12 | Maximize icon             |
| 5 | Log Out link   | 13 | Minimize icon             |
| 6 | About link   | 14 | Message Center            |
| 7 | Add Portlets icon  | 15 | Alarm Summary             |
| 8 | Change Layout icon   |    |                           |

## Adding a Portlet

Note the following about portlet management:

- By default, administrators can see all available portlets.
- Administrators can assign different portlets and layouts for each user role. The portlets are added automatically to a user's Prime Central home page.

- At first login, the user sees a set of portlets in a particular layout based on the logged-in user's role. The user can then customize the portlet selection and layout.

### Procedure

---

- Step 1** On the Prime Central home page, click the **Add Portlets** icon.
- Step 2** In the Add Portlets dialog box, click **Cisco Prime**.
- Step 3** Select the desired portlet and click **Add**. Alternatively, drag and drop the portlet to the desired location on the home page.  
You cannot add multiple instances of the same portlet to the home page.
- Step 4** Click the Close (**X**) icon to close the Add Portlets dialog box.
- 

## Maximizing or Minimizing a Portlet

### Procedure

---

- Step 1** Click the **Maximize** or **Minimize** icon in the top-right corner of the portlet.
- Step 2** To exit the view, do one of the following:
- In a maximized view, click the **Return to Home** icon in the top-right corner.
  - In a minimized view, click the **Restore** icon in the top-right corner. (The Minimize and Restore icons are toggle buttons.)
- 

## Removing a Portlet

### Procedure

---

- Step 1** In the top-right corner of the portlet, click the **Remove** icon.
- Step 2** At the confirmation prompt, click **OK**.
- 

## Adding or Removing Columns in a Portlet

### Procedure

---

- Step 1** In the top-right corner of the portlet, click the **Settings** icon.

**Note** Although the Alarm Browser and Alarm Report portlets do not have a Settings icon, you can customize their display. See [Changing the Alarm Information Displayed](#) and [Specifying the Report Order](#).

- Step 2** Click **Columns**. A list of all available columns in that portlet is displayed. Columns with a check mark are shown in the portlet; columns without a check mark are not shown in the portlet.
- Step 3** Uncheck the columns that you do not want displayed in the portlet. Check the columns that you want displayed.
- Step 4** Click **Close**.
- 

## Changing the Layout of the Home Page

Note the following layout constraints:

- Large portlets—such as User Management and Common Inventory—cannot be positioned together in a single row.
- Portlets are not rearranged automatically, unless you choose one of the following options:
  - Free (free-form)
  - 1 col (1 column)
- When a window is minimized or maximized, you cannot drag and drop portlets to rearrange them.
- If you choose the Free layout option, portlets are not aligned automatically; instead, you must rearrange them manually. In contrast with other layouts, the Free layout takes up the entire browser window instead of only the content area.

### Procedure

---

- Step 1** On the Prime Central home page, click the **Change Layout** icon.
- Step 2** Click the radio button that corresponds to the desired layout (one column, 50/50, and so on).
- Step 3** Click **Save**.
- 

## Changing the Time Zone

Prime Central stores events in the database in Coordinated Universal Time (UTC). The Prime Central portal converts events to the time zone that is configured on the client's workstation.

You can use the User Preferences portlet to change the default time zone used for time stamp displays.

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > System > User Preferences**.
- Step 2** In the User Preferences portlet, select a time zone from the Time Zone drop-down list.
- Time zone options are shown as offsets from UTC. The offset range is -11 to +14 hours from UTC.

**Note** The Language drop-down list is display only. U.S. English is the only language supported in Prime Central 1.5.3.

**Step 3** Click **Save**.

**Step 4** On the Prime Central home page, click the **Refresh Current Page** icon to see the time zone change.

---

## Changing the Prime Central Session Timeout

By default, the Prime Central session times out after 60 minutes of inactivity. You are prompted to extend the session 10 minutes before it times out. If you do not extend the session before the timeout, you are logged out automatically from Prime Central and from any applications.

When a session times out, the login window appears. When you log back in, you return to the Prime Central home page. It is recommended that you clear your browser cache and delete cookies before logging in again.

To change the default user session timeout, see [Configuring User Security Settings](#).

## Changing the Fault Management Session Timeout

By default, the Prime Central Fault Management session times out after 24 hours of inactivity. If you set the portal timeout to longer than 24 hours, you must change the Fault Management timeout to align with the portal timeout.

### Procedure

---

**Step 1** Log out of the Prime Central portal.

**Step 2** As the primeusr user, log in to the Prime Central Fault Management server.

**Step 3** Enter the following command to stop the server:

```
$NCHOME/fmctl stop
```

**Step 4** Open the `$NCHOME/tipv2/profiles/TIPProfile/config/cells/TIPCell/security.xml` file and locate the following section:

```
<authMechanisms xmi:type="security:LTPA" xmi:id="LTPA_1" OID="oid:1.3.18.0.2.30.2"
authContextImplClass="com.ibm.ISecurityLocalObjectTokenBaseImpl.
WSecurityContextLTPAImpl" authConfig="system.LTPA" simpleAuthConfig="system.LTPA"
authValidationConfig="system.LTPA" timeout="1440" keySetGroup="KeySetGroup_TIPNode_1">
```

**Step 5** Change the value of the timeout attribute as necessary. The default is 1440 minutes (24 hours).

**Note** If you have set up disaster recovery on another device, you must also make this change on that device.

**Step 6** Save and close the security.xml file.

**Step 7** Enter the following command to start the Prime Central Fault Management server:

```
$NCHOME/fmctl start
```

**Step 8** Log in to the Prime Central portal.

---

## Menu Structure

When you log in to Prime Central, the menu structure that you can access depends on your user privileges and which applications are installed and available. The following menus are visible to users with administrator-level privileges:

- [Home Menu](#)
- [Design Menu](#)
- [Fulfill Menu](#)
- [Assure Menu](#)
- [Analyze Menu](#)
- [Inventory Menu](#)
- [Administration Menu](#)



**Note** Although some browsers allow you to open multiple tabs within a single browser instance, you should not try to access the Prime Central portlets across multiple tabs within the same browser instance. You can, however, cross-launch to an application in a new browser tab.

## Home Menu

The Home menu (see the following figure) takes you to the Prime Central home page. When a portlet is maximized, the Return to Home icon returns you to the home page.

**Figure 4: Home Menu**



## Design Menu

From the Design menu (see the following figure), network designers can define the resources needed to build service profiles. Operators can then use these service profiles to fulfill service requests, provision, and activate the service.

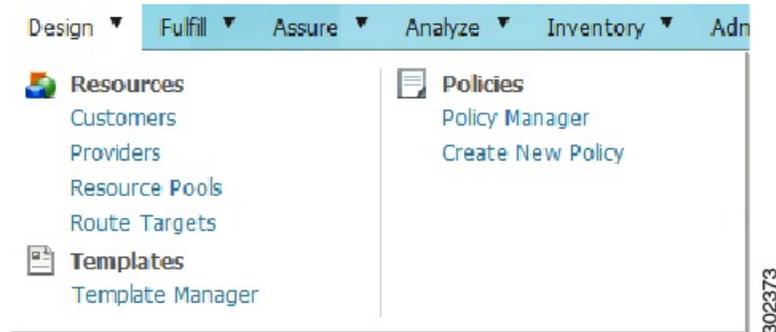
The Design menu cross-launches Prime Provisioning, where you can perform the following functions:

- **Customers**—Create and manage customers. A customer is typically an enterprise or large corporation that receives network services from a service provider.
- **Providers**—Create and manage provider accounts. A provider is typically a “service provider” or large corporation that provides network services to a customer.
- **Resource Pools**—Create and manage pools for IP address, multicast address, route distinguisher, site of origin, virtual circuit ID (VC ID), and VLAN.

- **Route Targets**—Create and manage route targets. A VPN can be organized into subsets called route targets, which describe how the customer edge (CE) router in a virtual private network (VPN) communicate with each other.
- **Template Manager**—Create and manage templates and associated data. Templates provide a means to deploy commands and configurations not normally supported by Prime Provisioning to a device. Templates are written in the Velocity Template Language (VTL) and are generally comprised of IOS and IOS XR device CLI configurations.
- **Policy Manager**—Create and manage policies for licensed services. Policies are used to define common tunnel attributes such as bandwidth pools, hold and setup priority, and affinity bits.
- **Create New Policy**—Create a new service policy, which can be applied to multiple provider edge (PE)-CE links in a single service request. A network operator defines service policies. A service operator uses a service policy to create service requests.

For details about using Prime Provisioning to provision your network, see the [Cisco Prime Provisioning 6.6 User Guide](#).

**Figure 5: Design Menu**



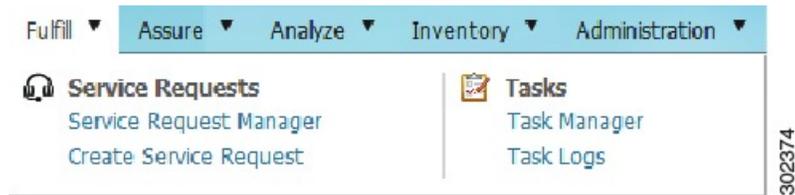
## Fulfill Menu

The Fulfill menu (see the following figure) cross-launches Prime Provisioning, where you can perform the following functions:

- **Service Request Manager**—Manage Prime Provisioning service requests.
- **Create Service Request**—Create a new Prime Provisioning service request.
- **Task Manager**—View pertinent information about current and expired tasks of all types, create and schedule new tasks, delete specified tasks, and delete the active and expired tasks.
- **Task Logs**—View task logs, which can be used to understand the status of a task, know whether it completed successfully, and troubleshoot why a task failed.

For details about Prime Provisioning service requests and tasks, see the [Cisco Prime Provisioning 6.6 User Guide](#).

Figure 6: Fulfill Menu

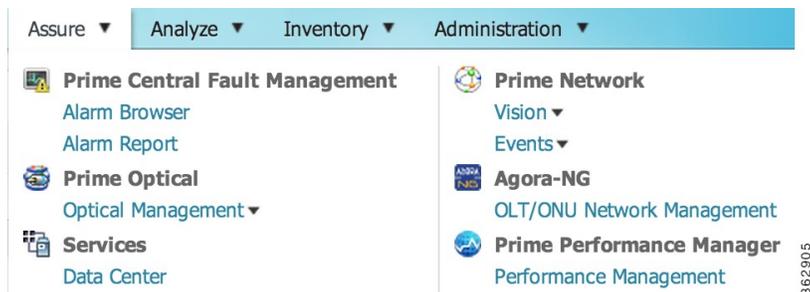


## Assure Menu

The Assure menu (see the following figure) contains the following menu options:

- Prime Central Fault Management—Cross-launches the following portlets that let you locate, diagnose, and report network problems:
  - Alarm Browser—See [Monitoring Affected Services and Customers](#).
  - Alarm Report—See [Analyzing Fault Data](#).
- Prime Optical > Optical Management—Cross-launches Prime Optical. If your network includes multiple instances of Prime Optical, you can choose which instance to launch. For details about using Prime Optical to manage your optical network, see the [Cisco Prime Optical 10.0 User Guide](#).
- Services > Data Center—Opens the Data Center portlet, where you can view information about data center compute services, network, and storage devices.
- Prime Network > Vision or Events—Cross-launches the selected Prime Network application. If your network includes multiple instances of Prime Network, you can choose which instance to launch. For details about using Prime Network to discover and manage your packet network, see the [Cisco Prime Network 4.1 User Guide](#).
- Agora-NG > OLT/ONU Network Management—Cross-launches the Cisco ME 4600 Series Agora-NG network provisioning platform. For more information, refer to this [datasheet](#).
- Prime Performance Manager > Performance Management—Cross-launches Prime Performance Manager. For details about using Prime Performance Manager to view the performance statistics and reports for a network, see the [Cisco Prime Performance Manager 1.5 User Guide](#).

Figure 7: Assure Menu

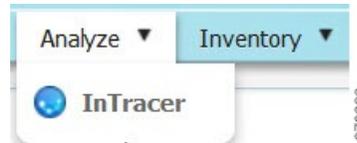


## Analyze Menu

The Analyze menu (see the following figure) cross-launches Cisco InTracer, a high-performance, subscriber troubleshooting and monitoring solution. It performs call tracing, control data acquisition, processing, and

analysis of both active and historical subscriber sessions. Cisco InTracer provides a framework for operators to analyze and investigate call flows and call events for subscriber sessions in near-real time. For more information about InTracer, see the [Cisco InTracer Installation and Administration Guide, Version 15.0](#).

**Figure 8: Analyze Menu**



## Inventory Menu

The Inventory menu (see the following figure) lets you view detailed inventory information for all devices in your network.

**Figure 9: Inventory Menu**

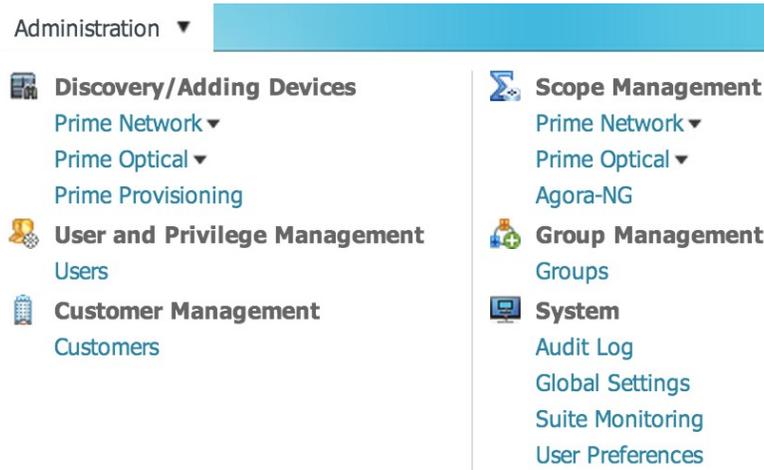


## Administration Menu

The Administration menu (see the following figure) contains the following menu options:

- Discovery/Adding Devices—Cross-launches Prime Network, Prime Optical, or Prime Provisioning. If your network includes multiple instances of Prime Network or Prime Optical, you can choose which instance to launch.
- User and Privilege Management > Users—Lets you perform user management operations, including defining users and passwords and configuring RBAC.
- Customer Management > Customers—Lets you add, edit, and delete customers; associate customers with network resources; disable and enable customer accounts; and export customer data.
- Scope Management—Lets you assign device scopes (in Prime Network and Agora-NG) or network elements (in Prime Optical) to Prime Central users. If your network includes multiple instances of Prime Network or Prime Optical, you can choose which instance to launch.
- Group Management > Groups—Lets you logically group network devices and services.
- System:
  - Audit Log—Lets you view user activity in Prime Central.
  - Global Settings—Lets you customize the terms-of-use message and configure when users see it.
  - Suite Monitoring—Lets you monitor Prime Central and the individual applications.
  - User Preferences—Lets you change the default time zone used for time stamp displays.

Figure 10: Administration Menu



362902

## Filtering and Searching

In some tables, the amount of detail can be overwhelming. In such cases, filtering helps eliminate unnecessary details, while searching helps you quickly locate data that you want to examine further.

By filtering a table's contents, you can view only those items that are of interest to you. This feature can be extremely helpful when working with tables that contain many entries.

### Filtering Using the Quick Filter

Most portlets have a Show drop-down list with a Quick Filter option, as shown in the following figure.

Figure 11: Quick Filter

Common Inventory

Synchronize Add to Group

|                          | Device Name    | Device Type                   | Status    | Alarms | Alarm Co. | Management IP Address |
|--------------------------|----------------|-------------------------------|-----------|--------|-----------|-----------------------|
| <input type="checkbox"/> | sol-M2-4       | Carrier Packet Transport 2... | Available |        | 24        | 209.165.200.224       |
| <input type="checkbox"/> | sanity-UCS     | Cisco UCS 6120XP              | Available |        | 0         | 209.165.200.225       |
| <input type="checkbox"/> | prime-cpt600-1 | Carrier Packet Transport 6... | Available |        | 10        | 209.165.200.226       |
| <input type="checkbox"/> | prime-cpt200-1 | Carrier Packet Transport 2... | Available |        | 8         | 209.165.200.227       |

#### Procedure

- Step 1** From the Show drop-down list, choose **Quick Filter**.

**Step 2** In the text field for each column, enter the search criteria.

**Note** In the Common Inventory portlet, the Quick Filter supports a percentage character (%) as a wildcard in the Management IP Address field. Other fields in the Common Inventory portlet do not use this character as a wildcard.

To search on complete octets in the Management IP Address field, the % character is not required. Instead, enter a period; the search returns the complete octet after the period.

## Filtering Using the Advanced Filter

Most portlets have a Show drop-down list with an Advanced Filter option, as shown in the following figure.

*Figure 12: Advanced Filter*

User Management

Users Groups Roles Privileges

Edit Delete Add Copy Reset Password Disable Enable

Match the following rule:

Filter   - + Go Clear Filter

|                          | Username     | First Name | Last Name | Roles | Groups          | Creation |
|--------------------------|--------------|------------|-----------|-------|-----------------|----------|
| <input type="checkbox"/> | centraladmin | admin      | admin     |       | PrimeAdminGroup | 2013-07  |

### Procedure

**Step 1** From the Show drop-down list, choose **Advanced Filter**.

**Step 2** Specify the required information for each criterion. For more information, see [Configuring an Advanced Filter Criterion](#).

**Step 3** Click the + icon to add another criterion for this filter.

**Step 4** Add additional criteria as required. To remove a criterion, click the - icon.

**Step 5** When you have specified all criteria for the filter, click **Go**.

The table data is displayed using the defined filter.

**Step 6** To clear a filter, click **Clear Filter**.

The table is refreshed and all entries are displayed.

## Configuring an Advanced Filter Criterion

The following table describes the actions you need to take when you configure an Advanced Filter criterion.

| Field  | Action/Description  |
|--|---|
| First drop-down list                               | Choose the primary match category. The drop-down list contains all columns in the current table.  |
| Second drop-down list                              | <p>Choose the rule to use for this criterion. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Contains</b>—The attribute value is returned if it contains the string you entered. The string can be located at the start, end, or middle of the attribute for the match to succeed. For example, if the string is <i>cle</i>, the following values match it in the <i>contains</i> mode: <i>clean</i>, <i>nucleus</i>, <i>circle</i>.</li> <li>• <b>Does not contain</b>—In this mode, only those attributes that do not contain the given string match. The results are opposite to that of the <i>contains</i> mode. For example, if you enter <i>cle</i> in this mode, <i>clean</i>, <i>nucleus</i>, and <i>circle</i> are rejected, but <i>foot</i> is deemed to match, because it does not contain <i>cle</i>.</li> <li>• <b>Starts with</b>—The value of the attribute must start with the string you entered. For example, if the string is <i>foot</i>, <i>footwork</i> matches, but <i>afoot</i> does not.</li> <li>• <b>Ends with</b>—This is the reverse of the <i>starts with</i> case, when a given attribute matches only if the specified string is at the end of the attribute value. In this mode, for example, the string <i>foot</i> matches <i>afoot</i> but not <i>footwork</i>.</li> <li>• <b>Is empty</b>—Lists the result where there is no value in the field.</li> <li>• <b>Is not empty</b>—Lists the result where the value is not missing from the field.</li> <li>• <b>Is exactly (or equals)</b>—This is the most generic mode, in which you can enter a full or partial expression that defines which nodes you are interested in.</li> <li>• <b>Does not equal</b>—Lists the result that does not equal the specified value.</li> <li>• <b>Is greater than</b>—Lists the result that is greater than the specified value.</li> <li>• <b>Is less than</b>—Lists the result that is less than the specified value.</li> <li>• <b>Is greater than or equal to</b>—Lists the result that is greater than or equal to the specified value.</li> <li>• <b>Is less than or equal to</b>—Lists the result that is less than or equal to the specified value.</li> </ul> |
| Third field (either drop-down list or entry field) | <p>The third field either lists the available values or allows you to enter text:</p> <ul style="list-style-type: none"> <li>• If a drop-down list is displayed, choose the required entry.</li> <li>• If an entry field is displayed, enter a string or regular expression for the criterion.</li> <li>• Any entry that is not a regular expression is treated as a string.</li> </ul>   |

## Sorting

To sort data in a table, simply click a column heading. By clicking the column heading, you can toggle between ascending and descending sort order. The column tooltip indicates whether the column is sortable, not sortable, or currently sorted.



**Note** You can sort only one column at a time.

A triangle next to the column heading indicates the sort order:

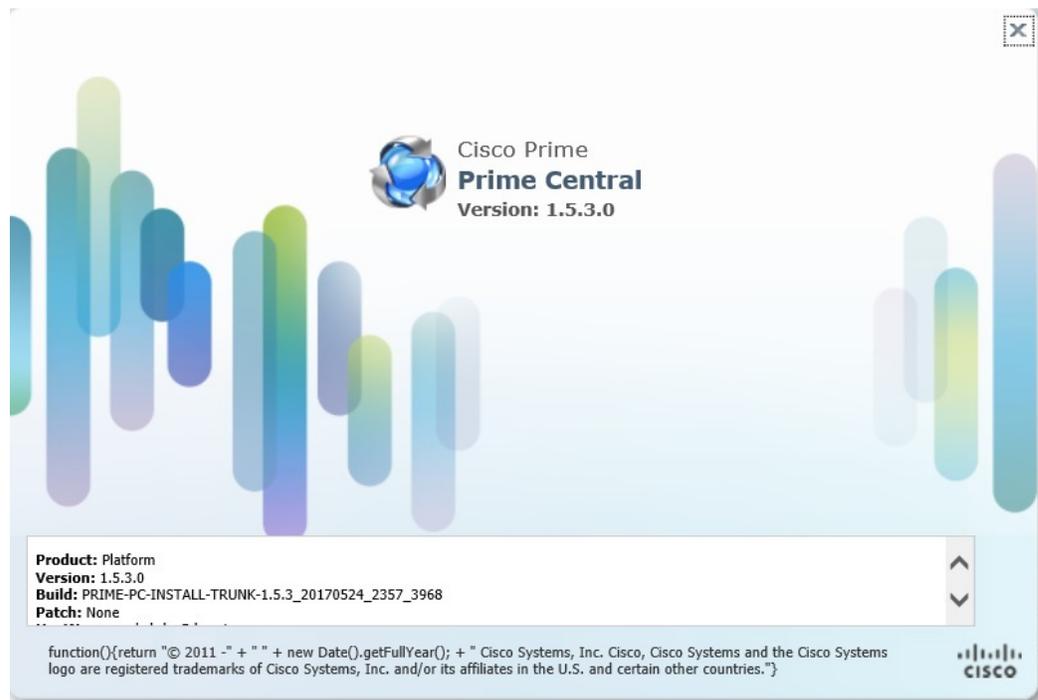
- indicates the column is sorted in ascending order.
- indicates the column is sorted in descending order.

## Finding the Prime Central Version

To find the Prime Central version you are running, click the **About** link on the portal home page.

The About window (see the following figure) displays the Prime Central version. Use the vertical scroll bar to view the Prime Central build and patch numbers, as well as version information for any installed applications.

**Figure 13: About Window**



## Logging Out of the Prime Central Portal

Prime Central features single sign-off. When you log out of the Prime Central portal home page, you are automatically logged out of any suite applications. If you cross-launched an application in a new browser tab or window, you must manually close that browser window after you log out of Prime Central.

### Closing the Prime Central Browser Without Logging Out

If your user account has a maximum number of active sessions (for example, one active session), and if you close your browser without logging out of Prime Central, your session is still in use, and you cannot log back in. When you try to log back in, the following error appears:

```
You are running the maximum number of allowed sessions for this user account.
Log out from one or more sessions and try again.
```

To restore your login, do the following:

- Check for the active sessions. If there is active sessions, then logout the first active user.
- Wait for the user session timeout (by default, 60 minutes), at which point your session expires. 10 minutes after expiration, all expired sessions are cleared automatically.
- Ask your system administrator to disable and then enable your user account in the User Management portlet. See [Enabling or Disabling a User Account](#).

## Managing the Self-Signed Certificates

When you log in to Prime Central for the first time, some browsers display a warning that the site is untrusted. When this happens, you must accept the self-signed, untrusted security certificates.

You can replace the Prime Central certificates in the following directories with your company's signed, trusted certificates.




---

**Note** For more detailed information on Managing the Self-Signed Certificates, refer to [Cisco Prime Central Managing Certificates](#).

---

## Importing an Existing Certificate into WebSphere

### Procedure

- 
- Step 1** On a supported browser, go to **<https://Fault-Management-server-IP-address:Fault-Management-web-service-listener-port/primefm/console>**.
- Note** The Prime Central Fault Management web service listener port is 16311.
- Step 2** Log in with the username and password that you configured for the Prime Central Fault Management application user during installation.
- Step 3** Choose **Settings > WebSphere Administrative Console > Launch WebSphere administrative console**.

- Step 4** From the left-pane menu bar in the Integrated Solutions Console tab, choose **Security > SSL certificate and key management**.
- Step 5** From the Related Items list in the center pane, choose **Key stores and certificates**.
- Step 6** From the table of keystores and certificates, choose the appropriate keystore. The default is NodeDefaultKeystore.
- Step 7** At the right of the Properties menu, choose **Personal certificates** from the Additional Properties list.
- Step 8** At the top of the certificates table, click the **Import** button.
- Step 9** From the General Properties menu, choose either **Managed key store** or **Key store file**, and fill out the required information for the option you chose. See the [Table 2: WebSphere General Properties Menu](#) for field descriptions.
- Step 10** Click **Apply** and **Save**.

## WebSphere General Properties Menu

The following table describes the WebSphere General Properties menu and the actions you need to take.

**Table 2: WebSphere General Properties Menu**

| Field                                      | Action  |
|--|---|
| Managed key store option                   | Imports the certificate from another keystore that is already being managed by the WebSphere Application Server. If you choose this option, do <i>not</i> : <ul style="list-style-type: none"> <li>• Enter a filename in the Key file name field</li> <li>• Select a format type from the Type drop-down list</li> <li>• Enter a password in the Key file password field</li> </ul> |
| Key store file option                      | Imports the certificate from a keystore contained in a file. If you choose this option, do <i>not</i> : <ul style="list-style-type: none"> <li>• Select a keystore from the Key store drop-down list</li> <li>• Enter a password in the Key store password field</li> </ul>   |
| Key store drop-down list                   | Choose a keystore to import.  |
| Key store password field                   | Enter the keystore password. The default password is <i>WebAS</i> .   |
| Key file name field                        | Enter the full filename of the keystore from which you want to import the certificate.  |
| Type drop-down list                        | Choose the format type of the certificate.  |
| Key file password field                    | Enter the key file password.  |
| Certificate alias to import drop-down list | Choose the alias for the certificate you want to import.  |
| Imported certificate alias field           | Enter an alias for the certificate in the keystore.   |

## Placing Certificates in the Internet Explorer Trusted Store

When you use Internet Explorer to log in to Prime Central, if you accept the security certificates without placing them in the trusted certificate store, they reappear upon subsequent logins.

To place certificates in the trusted store so they do not reappear upon subsequent logins:

### Internet Explorer 10 and 11

#### Procedure

---

- Step 1** With the Prime Central login window open, click **Certificate error** in the browser's address bar.  
The Untrusted Certificate dialog box opens.
- Step 2** Click **View certificates**.  
The Certificate dialog box opens.
- Step 3** Click **Install Certificate...** to launch the certificate import wizard.
- Step 4** Click **Next**.
- Step 5** Select the **Place all certificates in the following store** radio button option and then click **Browse...**
- Step 6** Navigate to the Trusted Root Certification Authorities folder and select it.
- Step 7** Click **OK**.
- Step 8** Click **Next**.
- Step 9** Click **Finish** to complete the wizard.  
A security warning appears.
- Step 10** Click **Yes** to confirm that you want to install the certificate.  
A message appears, indicating that the certificate import was successful.
- Step 11** Click **OK** to close the message.
- Step 12** Click **OK** to close the Certificate dialog box.
-



## CHAPTER 2

# Managing Users and Configuring Role-Based Access Control

This section describes how to manage users in Prime Central, including defining users and passwords and configuring role-based access control (RBAC).

Prime Central provides role-based access to various functions. Through RBAC, Prime Central allows a user to access some resources but not others, and to perform specific tasks based on the logged-in user's roles.

Authorization of tasks is controlled by user roles within Prime Central and user roles and scopes within the applications.

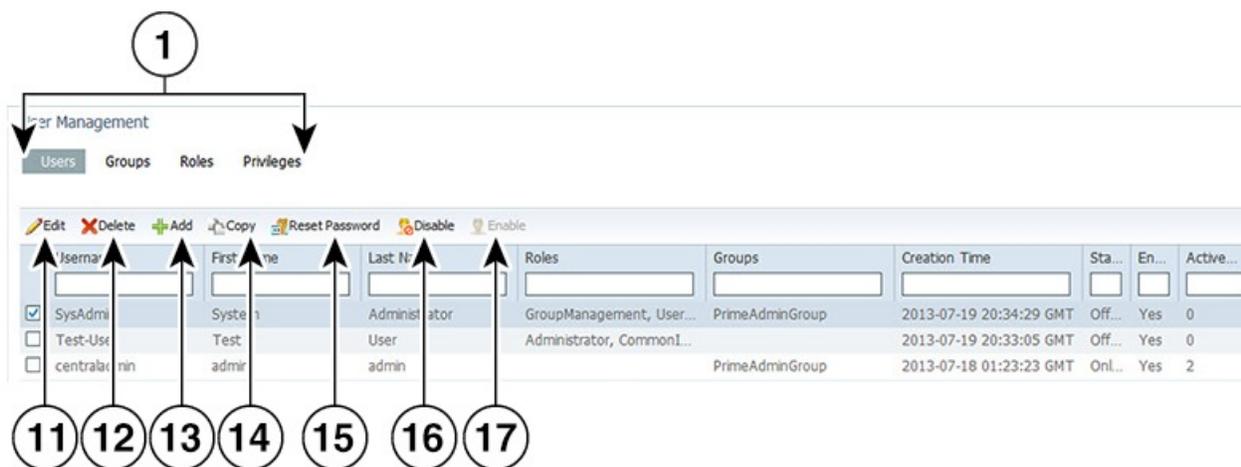
This section contains the following topics:

- [User Management Portlet, on page 23](#)

## User Management Portlet

The following figure shows the User Management portlet, where users with administrator-level privileges can perform all user management tasks.

**Figure 14: User Management Portlet**



|   |  |    |                     |
|---|--|----|---------------------|
| 1 | User management tabs: Users, Groups, Roles, Privileges | 10 | Properties pane     |
| 2 | Show drop-down list and Filter icon                    | 11 | Edit icon           |
| 3 | Number of selected table rows                          | 12 | Delete icon         |
| 4 | Total table rows                                       | 13 | Add icon            |
| 5 | Refresh icon   | 14 | Copy icon           |
| 6 | Export icon  | 15 | Reset Password icon |
| 7 | Settings icon  | 16 | Disable icon        |
| 8 | Options icon   | 17 | Enable icon         |
| 9 | Filter parameters area                                 | —  | —                   |

## Managing Users

You can add, edit, copy, and delete users; reset user passwords; disable and enable user accounts; and configure user security settings.

Each user can be assigned any number of roles, and each role can aggregate any number of privileges.

Prime Central includes a default user named *centraladmin* whose account cannot be deleted or disabled. The *centraladmin* user has local authentication, user management, and administrator privileges, but initially does not have any privileges on the various applications.

## Adding a User

### Procedure

- 
- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click **Add**.
- Step 3** In the Add User window:
- a) Enter general information about the new user, including username, first and last name, password, and email address. The variables that you define must adhere to the constraints described in [Name, Password, Phone, and Note Constraints](#).
 

The username is display only and cannot be changed.
  - b) For the **Local Authentication Fallback** check box:
    - If Prime Central is configured to use an external authentication provider such as TACACS+, RADIUS, or LDAP, check this check box to enable user authentication to fall back to the local Prime Central database when the external authentication server is unreachable.
    - If Prime Central is not configured to use external authentication, leave this check box unchecked. (It is unchecked by default.)

- c) (Optional) For the **Concurrent User Sessions** field, do one of the following:
- To have global user settings apply to the new user, click the Use Global Settings radio button. (For details about global settings, see [Configuring User Security Settings](#).)
  - To allow the user to open an unlimited number of concurrent Prime Central sessions, click the **Unlimited** radio button.
  - To limit the user to a specific number of concurrent sessions, click the **Number of Sessions** radio button and enter the desired number in the text box.
- d) (Optional) In the **Note** field, enter any notes for the user account.

**Step 4**

In the Application Access Privilege area, grant user access to the appropriate applications and assign individual roles:

- a) Select an application from the list of installed applications.

The list of roles specific to that application is displayed.

- b) Select the appropriate role for the user.

After you select a role, the Grant Access to *<application>* check box is checked automatically.

Note the following:

- When you add users, the status is displayed as Enable at the end of the operation. If you want to deactivate a user, use the **Update** option to deactivate a specific user.
- Prime Central includes a set of default roles for security and access control that allow different system functions. Click [Table 5: Default Prime Central Roles](#) to view a table which lists the default roles, the privileges that each role inherits, and the portlets that each role can access.
- The application access privilege and the user role are related. For example, if you assigned the user the Prime Central Fault Management access privilege, be sure to assign the user the Prime Central Fault Management role.
- You can assign the new user additional roles as desired.
- For Prime Central and Prime Provisioning, you can assign multiple roles to a user. For Prime Central Fault Management, Prime Network, Prime Optical, and Prime Performance Manager, you can assign only one role per user.
- If your network includes multiple instances of Prime Network or Prime Optical, the new user will be created on both application instances. For example, if you grant the new user access to Prime Optical and assign the user the SysAdmin role, that SysAdmin user will be created on both Prime Optical instances. However, if a Prime Optical instance is down when you add the new user, that SysAdmin user is not created on the Prime Optical instance until 5 minutes after the instance comes back up.
- When you grant a Prime Central user access to Agora-NG, you must assign the Agora-NG Administrator role to that user.

**Step 5**

Add the new user as a member of one or more groups:

- a) Select **Prime Central** from the installed applications list.
- b) Click the **Groups** tab.
- c) Check the check boxes for the appropriate groups.

All users that belong to the group share the same role.

**Step 6** Click **Add**.

The new user is displayed in the User Management portlet.

**Step 7** Assign device scopes (in Prime Network and Agora-NG) or NEs (in Prime Optical) to the new user:

- a) From the Prime Central menu, choose **Administration > Scope Management > Prime Network, Prime Optical, or Agora-NG**.
- b) Launch the appropriate application and assign device scopes or NEs to the new user. See the application documentation for details:
  - Prime Network—See "Creating New Device Scopes to Control Device Access" in the [Cisco Prime Network 5.0 Administrator Guide](#), Chapter 6, "Controlling Device Access and Authorization Using Device Scopes."
  - Prime Optical—See "Modifying a Prime Optical User's Properties" in the [Cisco Prime Optical 10.7 User Guide](#), Chapter 8, "Managing Security."
  - Agora-NG—See the following [datasheet](#).

---

## Name, Password, Phone, and Note Constraints

When adding, editing, or copying a user, the variables that you define must adhere to the constraints listed in the following table.

Table 3: Name, Password, Phone, and Note Constraints

| Variable                                 | Constraints  |
|--|--|
| Username                                 | <p>The username must:</p> <ul style="list-style-type: none"> <li>• Start with a letter.</li> <li>• Contain from 4 to 20 case-sensitive letters (A-Z, a-z), numbers (0-9), or hyphens (-), .</li> </ul> <p><b>Note</b> Prime Network and Prime Provisioning supports username with dot (.) whereas, Prime Performance Manager and Prime Optical does not support usernames with dot (.). Hence it is recommended not to carry out user operations with dot (.) in Prime Performance Manager and Prime Optical.</p> <ul style="list-style-type: none"> <li>• Not contain any other special characters or spaces.</li> <li>• Not be the reserved keywords <i>prime</i>, <i>web</i>, <i>guest</i>, <i>user</i>, <i>group</i>, <i>public</i>, or <i>private</i>, in any combination of uppercase or lowercase letters.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Usernames are case-sensitive. Prime Central treats <i>UserA</i> and <i>userA</i> as separate users.</li> <li>• If the username that you enter already exists in an installed application, Prime Central overwrites the existing application user with this new user.</li> </ul> |
| Group name, role name, or privilege name | <p>The name must:</p> <ul style="list-style-type: none"> <li>• Start with a letter.</li> <li>• Contain from 1 to 50 letters (A-Z, a-z), numbers (0-9), hyphens (-), or underscores (_).</li> <li>• Not contain spaces or other special characters.</li> </ul>  |

| Variable | Constraints   |
|----------|---|
| Password | <p>The password must:</p> <ul style="list-style-type: none"> <li>• Contain from 8 to 32 characters.</li> <li>• Not repeat the same character three or more times.</li> <li>• Contain characters from at least three of the following four classes: <ul style="list-style-type: none"> <li>• Uppercase letters (A-Z).</li> <li>• Lowercase letters (a-z).</li> <li>• Numbers (0-9).</li> <li>• Special characters.</li> </ul> </li> <li>• Not contain the username or the username in reverse.</li> <li>• Not contain <i>cisco</i>, <i>ocsic</i>, or any variation.</li> </ul> |
| Phone    | The phone number can contain up to 64 characters. All characters are allowed.   |
| Note     | The note can contain up to 1000 characters. All characters are allowed.   |

## User Information in the Quick View

In the User Management portlet, the quick view displays additional user information when the cursor rests over the icon shown in the following figure.

Figure 15: Quick View of Additional User Details

The screenshot shows the 'User Management' interface. On the left, there is a list of users: 'SysAdmin', 'Test-User', and 'centraladmin'. The 'centraladmin' user is selected, and an arrow points to a plus icon next to it. On the right, the 'User Details' panel is expanded, showing the following information:

|                                    |  |
|------------------------------------|--|
| Phone                              |  |
| Email                              | admin@xmp.com                                  |
| Local Authentication Fallback Note | Enabled  |
| Application Role                   | Prime Central Fault Management Administrator   |
| Application Role                   | Prime Provisioning SysAdminRole                |
| Application Role                   | Prime Performance Manager System Administrator |
| Application Role                   | Prime Network Administrator                    |
| Application Role                   | Prime Optical SuperUser                        |

## Editing a User

### Procedure

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, select the user that you want to edit and click **Edit**.
- Step 3** In the Edit User window:
- Edit the user's first or last name, email address, or phone number, as required. The variables that you define must adhere to the constraints described in [Name, Password, Phone, and Note Constraints](#).  
The username is display only and cannot be changed.
  - For the **Local Authentication Fallback** check box:
    - If Prime Central is configured to use an external authentication provider such as TACACS+, RADIUS, or LDAP, check this check box to enable user authentication to fall back to the local Prime Central database when the external authentication server is unreachable.
    - If Prime Central is not configured to use external authentication, leave this check box unchecked. (It is unchecked by default.)

- c) (Optional) For the Concurrent User Sessions field, do one of the following:
- To have global user settings apply to the new user, click the **Use Global Settings** radio button. (For details about global settings, see [Configuring User Security Settings](#).)
  - To allow the user to open an unlimited number of concurrent Prime Central sessions, click the **Unlimited** radio button.
  - To limit the user to a specific number of concurrent sessions, click the **Number of Sessions** radio button and enter the desired number in the text box.
- d) (Optional) In the Note field, enter any notes for the user account.

**Step 4** In the Application Access Privilege area, click the **Roles** tab and update the user's application access and roles, as required. If an application is not installed, it is not listed here.

Note the following:

- Application access and roles (except Prime Central roles) are all that you can edit for the *centraladmin* user.
- The application access privilege and the user role are related. For example, if you assigned the user the Prime Central Fault Management access privilege, be sure to assign the user the Prime Central Fault Management role.
- For Prime Central, all users are assigned the User role automatically. You can assign the user additional roles as desired.
- For Prime Central and Prime Provisioning, you can assign multiple roles to a user. For Prime Central Fault Management, Prime Network, Prime Optical, and Prime Performance Manager, you can assign only one role per user.
- If your network includes multiple instances of Prime Network or Prime Optical, the user will be created on both application instances. For example, if you grant the user access to Prime Optical and assign the user the SysAdmin role, that SysAdmin user will be created on both Prime Optical instances. However, if a Prime Optical instance is down when you add the user, that SysAdmin user is not created on the Prime Optical instance until 5 minutes after the instance comes back up.

**Step 5** In the Application Access Privilege area, click the **Groups** tab and update the user's assigned groups and group roles, as required.

**Step 6** Click **Update**. The updated user is displayed in the User Management portlet..

If you changed a user's assigned roles or access privileges, that user must log out of Prime Central and log back in to see the changes. The changes do not take effect until the user logs in next.

You can also use **Update** to deactivate an user.

**Step 7** (Optional) Reassign device scopes to the user you edited:

- a) From the Prime Central menu, choose **Administration > Scope Management > Prime Network** or **Prime Optical**.
- b) Launch the appropriate application and reassign device scopes or NEs to the user. See the application documentation for details:
  - Prime Network—See "Creating New Device Scopes to Control Device Access" in the [Cisco Prime Network 5.0 Administrator Guide](#), Chapter 6, "Controlling Device Access and Authorization Using Device Scopes."

- Prime Optical—See "Modifying a Prime Optical User's Properties" in the [Cisco Prime Optical 10.7 User Guide](#), Chapter 8, "Managing Security."

---

## Copying a User

You can easily create a new user by copying an existing user's assigned privileges, groups, and roles.

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, select the user that you want to copy and click **Copy**.
- Step 3** In the Add User window, make the following entries (this information is unique to each user and is therefore not copied from the existing user):
- a) Specify a username, first and last name, password, email address, and phone number. See the constraints described in [Name, Password, Phone, and Note Constraints](#).
  - b) For the **Local Authentication Fallback** check box:
    - If Prime Central is configured to use an external authentication provider such as TACACS+, RADIUS, or LDAP, check this check box to enable user authentication to fall back to the local Prime Central database when the external authentication server is unreachable.
    - If Prime Central is not configured to use external authentication, leave this check box unchecked. (It is unchecked by default.)
  - c) (Optional) For the **Concurrent User Sessions** field, do one of the following:
    - To have global user settings apply to the new user, click the **Use Global Settings** radio button. (For details about global settings, see [Configuring User Security Settings](#).)
    - To allow the user to open an unlimited number of concurrent Prime Central sessions, click the **Unlimited** radio button.
    - To limit the user to a specific number of concurrent sessions, click the **Number of Sessions** radio button and enter the desired number in the text box.
  - d) (Optional) In the Note field, enter any notes for the user account.
- Step 4** For each of the following items, make any changes needed for the new user (the current information is copied from the existing user):
- Application access
  - User roles
  - Groups and group roles
- Step 5** Click **Add**.
- The new user is displayed in the User Management portlet.
- Step 6** Assign device scopes (in Prime Network and Agora-NG) or NEs (in Prime Optical) to the new user:

- a) From the Prime Central menu, choose **Administration > Scope Management > Prime Network, Prime Optical, or Agora-NG**.
- b) Launch the appropriate application and assign device scopes or NEs to the new user. See the application documentation for details:
  - Prime Network—See "Creating New Device Scopes to Control Device Access" in the [Cisco Prime Network 5.0 Administrator Guide](#), Chapter 6, "Controlling Device Access and Authorization Using Device Scopes."
  - Prime Optical—See "Modifying a Prime Optical User's Properties" in the [Cisco Prime Optical 10.7 User Guide](#), Chapter 8, "Managing Security."
  - Agora-NG—See the following [datasheet](#).

## Deleting a User

### Procedure

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, select the user that you want to delete and click **Delete**.
- Step 3** At the confirmation prompt, click **Yes**.

If the user exists on an application that is down when you delete the user from Prime Central, that user will persist on that particular application as a local user.

## Resetting Another User's Password

Users with administrator-level privileges can reset another user's password.

### Procedure

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, select the user whose password you want to reset and click **Reset Password**.
- Step 3** In the Reset Password dialog box, enter a new password that adheres to the constraints described in [Name, Password, Phone, and Note Constraints](#).
- Step 4** Enter the new password again to confirm the entry.
- Step 5** Click **Save**.

## Resetting Your User Password

Users of any privilege level can use the My Account portlet to reset their own Prime Central password. The password reset applies to the Prime Central user who is currently logged in.

## Procedure

- Step 1** On the portal home page, place your cursor over your login name (to the left of the Log Out link) and click **My Account**. In the example shown in the following figure, the name is *Test User*.
- Step 2** In the My Account portlet, enter your current password in the Current Password field.
- Step 3** In the New Password field, enter a new password that adheres to the constraints described in [Name, Password, Phone, and Note Constraints](#).
- Step 4** Enter the new password again to confirm the entry.
- Step 5** (Optional) In the Email field, edit the email address that will be displayed in the User Management portlet. This field is dimmed for the *centraladmin* user.
- Step 6** (Optional) In the Phone field, edit the phone number that will be displayed in the User Management portlet. This field is dimmed for the *centraladmin* user.
- Step 7** Click **Save**.

**Figure 16: My Account Portlet**

The screenshot shows the 'My Account' portlet in the Cisco Prime Central interface. The portlet title is 'My Account'. The form contains the following fields:

- \* Current Password: [password field]
- New Password: [password field]
- \* Confirm New Password: [password field]
- \* Email: test@cisco.com
- Phone: 408 555-1212

At the bottom right of the form, there are two buttons: 'Save' and 'Reset'.

## Resetting a Lost Password

From the UNIX command line, the Linux root user on the Prime Central portal can reset any Prime Central portal user's password, including an administrator password.

Complete this procedure only after trying [Resetting Another User's Password](#) and [Resetting Your User Password](#).

### Procedure

- Step 1** As the primeusr user, log in to the Prime Central portal with the primeusr password that you specified during installation.
- Step 2** Enter the following command:  
**su root**

**Step 3** When prompted, enter the root user password.

**Step 4** Change directories to the \$XMP\_HOME/bin folder.

**Step 5** Enter the following command:

```
resetUserPassword.ksh
```

**Step 6** When prompted, enter the Prime Central username and the new password. In the following example, the Prime Central username is *User\_XYZ*

```
Please enter username:
User_XYZ
Please enter new password:
Please enter confirm password:
```

When the script finishes, output similar to the following is displayed:

```
Loading USER - User_XYZ
Validating new password..
Resetting password ..
Resetting password COMPLETED.
EXECUTION STATUS : Success
```

---

## Enabling or Disabling a User Account

Users with administrator-level privileges can enable or disable another user's account. However, you cannot disable the *centraladmin* user account.

### Procedure

**Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.

**Step 2** In the User Management portlet, select the desired user and click **Enable** or **Disable**.

The User Management portlet > Enabled column displays the following value:

- Yes—The user is enabled and can log in to Prime Central.
- No—The user is disabled and cannot log in to Prime Central.

---

## Configuring User Security Settings

Users with the appropriate privileges can configure security settings that apply to all other users.

The following security settings do not apply to the *centraladmin* user, who has administrator-level privileges:



### Note

- Maximum Log In Attempts
- Maximum Active User Sessions
- User Inactivity Period Before Deactivation (days)
- User Inactivity Deactivation Mode

**Procedure**

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the top-right corner of the User Management portlet, click the **Options** icon.
- Step 3** Click the **Configuration** link. The User Management - Configuration dialog box (see the following figure) opens.
- Step 4** Configure the security settings that will apply to all users. See the [Table 4: User Security Setting Descriptions](#) table for more information.
- Step 5** Click **Save**.

*Figure 17: User Management - Configuration Dialog Box*

**User Management - Configuration**

Maximum Log In Attempts:

Maximum Active User Sessions:

User Session Timeout (minutes):

Password Expiration (days):

Password Expiration Warning (days):

Number of Passwords Before Reuse:

Used Password Re-enablement Period (days):

Minimum Duration Between Password Change (days):

Number of Prohibited Consecutive Characters From Previous Password:

Reset Password after User Creation:  Enable  
 Disable

User Inactivity Period Before Deactivation (days):

User Inactivity Deactivation Mode:  Disable Account  
 Delete Account

**User Security Setting Descriptions**

The following table describes the security settings you can configure for the users in your network.

Table 4: User Security Setting Descriptions

| Setting  | Description   |
|--|---|
| Maximum Log In Attempts  | The maximum number of failed login attempts allowed before the user account is denied access to Prime Central. The default is 6 retries.  |
| Maximum Active User Sessions                                       | The number of concurrent sessions allowed. The default is 1 session.  |
| User Session Timeout (minutes)                                     | The number of minutes a user's session is inactive before Prime Central automatically locks the user out. By default, the session times out after 60 minutes of inactivity. You are prompted to extend the session 10 minutes before it times out. If you do not extend the session before the timeout, you are logged out automatically from Prime Central and from any applications.  |
| Password Expiration (days)   | The number of days before the password expires. The default is 60 days.   |
| Password Expiration Warning (days)                                 | The early warning period for password expiration. The default is 10 days. The value in this field must be less than the value in the Password Expiration field.   |
| Number of Passwords Before Reuse                                   | <p>The number of different passwords a user must use before being allowed to reuse the first password. The default is 4 passwords.</p> <p>This field takes priority over the Used Password Re-enablement Period field. For example, assume that:</p> <ul style="list-style-type: none"> <li>• Number of Passwords Before Reuse: 2</li> <li>• Used Password Re-enablement Period: 5</li> </ul> <p>If the user password is <i>test</i>, you can change it to <i>sample</i> the next day, and then to <i>basic</i> on the second day. You can then change it back to <i>test</i> before 5 days elapses, because the Number of Passwords Before Reuse field takes priority.</p> |
| Used Password Re-enablement Period (days)                          | The number of days before an old password can be reused. The default is 120 days.   |
| Minimum Duration Between Password Change (days)                    | The number of days a user must wait between password changes. The default is 0 days.  |
| Number of Prohibited Consecutive Characters From Previous Password | The number of consecutive characters by which the new password must differ from the previous one. The default is 3 characters.  |
| Reset Password after User Creation                                 | Specify whether newly added users will be prompted to reset their password before their first login.  |
| User Inactivity Period Before Deactivation (days)                  | The number of days a user's session is inactive before Prime Central automatically deactivates the user. The default is 30 days.  |
| User Inactivity Deactivation Mode                                  | Specify whether to disable or delete an inactive user account. The default is <i>Disable Account</i> .  |

## Managing Groups

All users that belong to a particular group share the same role and have access to a specific set of functions. User groups can be tied to one or more roles. The idea is to easily create groups of users who all share the same access privileges. A user can be assigned to more than one group, but this is not typical, as a single group should define an overall operational role within the suite.

Prime Central includes a default group named *PrimeAdminGroup* that cannot be edited or deleted.

### Adding a Group

#### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Groups** tab.
- Step 3** Click **Add**.
- Step 4** In the Add Group dialog box:
- Enter a group name that conforms to the constraints listed in the [Table 3: Name, Password, Phone, and Note Constraints](#) table.
  - Enter a description that contains from 1 to 50 alphanumeric or special characters.
  - Check the appropriate role check boxes to assign the new group at least one role.
  - Click **Add**.

The new group is displayed in the Groups tab.

---

### Editing a Group

#### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Groups** tab.
- Step 3** Select the group that you want to edit and click **Edit**.
- Step 4** Edit the group description or assigned roles, as required. The group description can contain from 1 to 50 alphanumeric or special characters.
- The group name is display only and cannot be changed.
- Step 5** Click **Update**.
-

## Deleting a Group

### Procedure

- 
- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Groups** tab.
- Step 3** Select the group that you want to delete and click **Delete**.
- Step 4** At the confirmation prompt, click **Yes**.
- 

## Managing Roles

Users have access to functions based on the role to which they are assigned. Roles define the functions or tasks a user can perform. A user can be assigned more than one role.

Prime Central includes a set of default roles for security and access control that allow different system functions. The following table lists the default roles, the privileges that each role inherits, and the portlets that each role can access. (The default privileges are explained in [Managing Privileges](#).) The default roles cannot be edited or deleted.

User roles inherit privileges as a union of role types. For example, the Fault Management role (which has no Common Inventory access) paired with the User role (which has Common Inventory access) results in Common Inventory access.

*Table 5: Default Prime Central Roles*

| Default Role Name | Privileges                | Ability to Access These Portlets: |                  |                 |                  |                  |                  |               |              |           |
|-------------------|---------------------------|-----------------------------------|------------------|-----------------|------------------|------------------|------------------|---------------|--------------|-----------|
|                   |                           | My Account                        | User Preferences | User Management | Suite Monitoring | Group Management | Common Inventory | Alarm Browser | Alarm Report | Audit Log |
| Administrator     | Admin Privilege           | Yes                               | Yes              | Yes             | Yes              | Yes              | Yes              | Yes           | Yes          | Yes       |
|                   | All Access Privilege      |                                   |                  |                 |                  |                  |                  |               |              |           |
|                   | InTracer Launch Privilege |                                   |                  |                 |                  |                  |                  |               |              |           |

| Default Role Name      | Privileges                         | Ability to Access These Portlets: |                  |                 |                  |                  |                  |               |              |           |
|------------------------|------------------------------------|-----------------------------------|------------------|-----------------|------------------|------------------|------------------|---------------|--------------|-----------|
|                        |                                    | My Account                        | User Preferences | User Management | Suite Monitoring | Group Management | Common Inventory | Alarm Browser | Alarm Report | Audit Log |
| Common Inventory Admin | Common Inventory Admin Privilege   | Yes                               | Yes              | No              | Yes              | No               | Yes              | No            | No           | No        |
|                        | Cross Launch Privilege             |                                   |                  |                 |                  |                  |                  |               |              |           |
|                        | Subsystem Inventory User Privilege |                                   |                  |                 |                  |                  |                  |               |              |           |
|                        | User Privilege                     |                                   |                  |                 |                  |                  |                  |               |              |           |
| Common Inventory User  | Common Inventory User Privilege    | Yes                               | Yes              | No              | Yes              | No               | Yes              | No            | No           | No        |
|                        | Cross Launch Privilege             |                                   |                  |                 |                  |                  |                  |               |              |           |
|                        | Subsystem Inventory User Privilege |                                   |                  |                 |                  |                  |                  |               |              |           |
|                        | User Privilege                     |                                   |                  |                 |                  |                  |                  |               |              |           |
| Fault Management       | Cross Launch Privilege             | Yes                               | Yes              | No              | Yes              | No               | No               | Yes           | Yes          | No        |
|                        | Fault Management Privilege         |                                   |                  |                 |                  |                  |                  |               |              |           |
|                        | Subsystem Inventory User Privilege |                                   |                  |                 |                  |                  |                  |               |              |           |
|                        | User Privilege                     |                                   |                  |                 |                  |                  |                  |               |              |           |

| Default Role Name     | Privileges                          | Ability to Access These Portlets: |                  |                 |                  |                  |                  |               |              |           |
|-----------------------|-------------------------------------|-----------------------------------|------------------|-----------------|------------------|------------------|------------------|---------------|--------------|-----------|
|                       |                                     | My Account                        | User Preferences | User Management | Suite Monitoring | Group Management | Common Inventory | Alarm Browser | Alarm Report | Audit Log |
| Group Management      | Group Management Privilege          | Yes                               | Yes              | No              | No               | Yes              | No               | No            | No           | No        |
|                       | User Privilege                      |                                   |                  |                 |                  |                  |                  |               |              |           |
| User                  | Common Inventory User Privilege     | Yes                               | Yes              | No              | Yes              | No               | Yes              | Yes           | Yes          | No        |
|                       | Cross Launch Privilege              |                                   |                  |                 |                  |                  |                  |               |              |           |
|                       | Fault Management Privilege          |                                   |                  |                 |                  |                  |                  |               |              |           |
|                       | Subsystem Inventory User Privilege  |                                   |                  |                 |                  |                  |                  |               |              |           |
|                       | User Privilege                      |                                   |                  |                 |                  |                  |                  |               |              |           |
| User Management Admin | Cross Launch Privilege              | Yes                               | Yes              | Yes             | Yes              | No               | No               | No            | No           | No        |
|                       | Subsystem Inventory Admin Privilege |                                   |                  |                 |                  |                  |                  |               |              |           |
|                       | User Privilege                      |                                   |                  |                 |                  |                  |                  |               |              |           |
|                       | User Management Admin Privilege     |                                   |                  |                 |                  |                  |                  |               |              |           |



**Note** In the GUI, there are no spaces in the role or privilege names.

## Adding a Role

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Roles** tab.
- Step 3** Click **Add**.
- Step 4** In the Add Role dialog box:
- Enter a role name that conforms to the constraints listed in the [Table 3: Name, Password, Phone, and Note Constraints](#) table.
  - Enter a description that contains from 1 to 50 alphanumeric or special characters.
  - Check the appropriate privilege check boxes to assign the new role at least one privilege. Prime Central provides the default privileges listed in [Managing Privileges](#).
  - Click **Add**.
- The new role is displayed in the Roles tab.
- 

## Editing a Role

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Roles** tab.
- Step 3** Select the role that you want to edit and click **Edit**.
- Step 4** Edit the role description or assigned privileges, as required. The role description can contain from 1 to 50 alphanumeric or special characters.
- The role name is display only and cannot be changed.
- Step 5** Click **Update**.
- 

## Deleting a Role

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Roles** tab.
- Step 3** Select the role that you want to delete and click **Delete**.
- Step 4** At the confirmation prompt, click **Yes**.
-

## Managing Privileges

Privileges control the portlets, menu options, and back-end URLs that a role is authorized to access in Prime Central.

Prime Central provides the default privileges shown in the following table. The default privileges cannot be edited or deleted.

**Table 6: Default Prime Central Privileges**

| Default Privilege Name              | Can...   |
|-------------------------------------|--|
| Admin Privilege                     | <ul style="list-style-type: none"> <li>Issue all back-end operations, including create, read, update, and delete (CRUD).</li> </ul>  |
| All Access Privilege                | <ul style="list-style-type: none"> <li>See all menu options.</li> </ul>  |
| Common Inventory Admin Privilege    | <ul style="list-style-type: none"> <li>Access the Common Inventory portlet.</li> <li>Access the Suite Monitoring portlet.</li> <li>Issue all common inventory back-end operations, including CRUD.</li> </ul>  |
| Common Inventory User Privilege     | <ul style="list-style-type: none"> <li>Issue GET ONLY common inventory back-end operations.</li> <li>Access the Common Inventory portlet.</li> <li>Access the Suite Monitoring portlet.</li> </ul>   |
| Cross Launch Privilege              | <ul style="list-style-type: none"> <li>Cross-launch applications.</li> </ul>   |
| Fault Management Privilege          | <ul style="list-style-type: none"> <li>Access the Alarm Browser portlet.</li> <li>Access the Alarm Report portlet.</li> <li>Access the Suite Monitoring portlet.</li> </ul>  |
| Group Management Privilege          | <ul style="list-style-type: none"> <li>Access the Group Management portlet.</li> <li>See the following menu option:<br/>Administration &gt; Group Management &gt; Groups</li> <li>Issue all group management back-end operations, including CRUD.</li> </ul> |
| InTracer Launch Privilege           | <ul style="list-style-type: none"> <li>Cross-launch the InTracer application.</li> </ul>   |
| Subsystem Inventory Admin Privilege | <ul style="list-style-type: none"> <li>Issue all subsystem inventory back-end operations, including CRUD.</li> <li>Access the Suite Monitoring portlet.</li> </ul>   |
| Subsystem Inventory User Privilege  | <ul style="list-style-type: none"> <li>Issue GET ONLY subsystem inventory back-end operations.</li> </ul>  |

| Default Privilege Name          | Can...   |
|---------------------------------|--|
| User Management Admin Privilege | <ul style="list-style-type: none"> <li>• Issue all user management back-end operations, including CRUD.</li> <li>• Access the User Management portlet.</li> <li>• Access the Suite Monitoring portlet.</li> </ul>  |
| User Privilege                  | <ul style="list-style-type: none"> <li>• See most menu options, <i>except for the following</i>: <ul style="list-style-type: none"> <li>• Assure &gt; Prime Fault Management &gt; Alarm Browser</li> <li>• Assure &gt; Prime Fault Management &gt; Alarm Report</li> <li>• Inventory &gt; Common Inventory &gt; Devices</li> <li>• Administration &gt; User and Privilege Management &gt; Users</li> <li>• Administration &gt; System &gt; Suite Monitoring</li> </ul> </li> <li>• Access the My Account portlet.</li> <li>• Access the User Preferences portlet.</li> </ul> |



**Note** In the GUI, there are no spaces in the privilege names.

## Adding a Privilege

### Procedure

- 
- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Privileges** tab.
- Step 3** Click **Add**.
- Step 4** In the Add Privilege window:
- Enter a privilege name that conforms to the constraints listed in the [Table 3: Name, Password, Phone, and Note Constraints](#) table.
  - Enter a description that contains from 1 to 50 alphanumeric or special characters.
  - In the URL Filter Expression field, enter a URL filter expression to enable access to a specific back-end URL pattern. This field is a free-form text field; all characters are allowed.
  - Assign portlets to the privilege by checking the appropriate check boxes.
  - Select which menu options the privilege will be able to access. Click the Expand icon and navigate to the appropriate menu options.
- Step 5** Click **Add**.
- Step 6** Create a new role and assign it the newly created privilege in the Privileges tab. See [Adding a Role](#).
-

## Editing a Privilege

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
  - Step 2** In the User Management portlet, click the **Privileges** tab.
  - Step 3** Select the privilege that you want to edit and click **Edit**.
  - Step 4** In the Edit Privilege window, update the privilege description, URL filter expressions, assigned portlets, and menu options, as required. The description can contain from 1 to 50 alphanumeric or special characters.  
The privilege name is display only and cannot be changed.
  - Step 5** Click **Update**.
- 

## Deleting a Privilege

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
  - Step 2** In the User Management portlet, click the **Privileges** tab.
  - Step 3** Select the privilege that you want to delete and click **Delete**.
  - Step 4** At the confirmation prompt, click **Yes**.
- 

## Creating a Bulk User

From the Unix command line, you can create a new user named 'bulkuser' that can be used for Bulk User management operations.

### Procedure

---

- Step 1** Log in to the Prime Central as a root user.
  - Step 2** In the directory *installation-directory/utills/prime\_tools/UtilityUsersDir* folder, run the *./createBulkUser* script.  
A user with name 'bulkuser' is created, which can be used for BulkUser Management operations.
- 

## Importing Users in Bulk

From the UNIX command line, you can perform a bulk import of users from an Excel file that you create.

## Procedure

**Step 1** As the *bulkuser* user, log in to the Prime Central server with the *bulkuser* password that you specified during creation.

**Step 2** Change directories to the *installation-directory/utls/prime\_tools/UtilityUsersDir* folder.

**Step 3** Create your own Excel file that contains all the users you want to import; then, add that spreadsheet to the *UtilityUsersDir* folder.

By default, the *UtilityUsersDir* folder contains a sample spreadsheet named *customers.xlsx*. You can structure your Excel file similarly.

The sample *customers.xls* file contains four sheets, each of which corresponds to a step in the User Management portlet > Add wizard.

Each sheet contains a GLOBAL SETTING row with information that will apply to all users, unless you overwrite the global setting with your specified value. If you leave a cell blank, Prime Central uses the global setting.

**Note** While creating users, it is recommended to use system generated passwords or the password given by *bulkuser*. Keeping passwords in spreadsheet may lead to security vulnerabilities.

**Step 4** Enter the following command to import the users defined in your Excel file into the Prime Central database:

```
sh importUsers FILE -c Excel-filename
```

For example, to import a file named *users\_xyz.xlsx*, enter:

```
sh importUsers FILE -c users_xyz.xlsx
```

**Step 5** At the following prompt, enter your Prime Central administrative username and password:

```
Enter Prime Central admin username:
Enter Prime Central admin user password:
```

**Step 6** At the following prompt:

```
Do you want the system to generate a random password for each imported user? [Y|N]:
```

Enter one of the following:

- **Y** if you want Prime Central to generate a random password for each imported user, unless overwritten by your Excel file.
- **N** if you want to choose a default password for all imported users. Then, at the following prompt, enter a password that will apply to all users.

```
Enter a default password for all imported users:
```

The import begins. After Import, output similar to the following is displayed:

```
User USER_3 is created successfully in Prime Central with local password password
User USER_2 is created successfully in Prime Central with local password password
User USER_1 is created successfully in Prime Central with local password password
Number of users requested: 3
Number of users imported: 3
```

**Note** You cannot import the same username more than once. If you try to import multiple users with the same username, Prime Central returns the following error: “User *username* already exists in Prime Central.”

When you add users, in the **User Management** window, **Yes** is displayed by default in the **Enabled** column at the end of the operation. If you want to deactivate a user, use the **Update** option to deactivate a specific user. After you deactivate a user the status is displayed as **No** in the Enabled column.

**Step 7** Log in to Prime Central and choose **Administration > User and Privilege Management > Users** to open the User Management portlet. Verify that the users you imported are visible in the **Users** tab.

For the imported users, roles associated to bulk users, their associated groups and relevant domain managers from an Excel file that you create will be assigned automatically.

## Updating Users in Bulk

From the UNIX command line, you can perform a bulk update of users from an Excel file that you create.

### Procedure

**Step 1** As the *bulkuser* user, log in to the Prime Central server with the bulkuser password that you specified during creation.

**Step 2** Change directories to the *installation-directory/utls/prime\_tools/UtilityUsersDir* folder.

**Step 3** Create your own Excel file that contains all the users you want to update; then, add that spreadsheet to the UtilityUsersDir folder.

By default, the UtilityUsersDir folder contains a sample spreadsheet named *customers.xlsx*. You can structure your Excel file similarly.

The sample *customers.xls* file contains four sheets, each of which corresponds to a step in the User Management portlet > Add wizard.

Each sheet contains a GLOBAL SETTING row with information that will apply to all users, unless you overwrite the global setting with your specified value. If you leave a cell blank, Prime Central uses the global setting.

**Step 4** Enter the following command to update the users defined in your Excel file into the Prime Central database:

```
sh importUsers-u FILE Excel-filename
```

For example, to update a file named *users\_xyz.xlsx*, enter:

```
sh importUsers-u FILE users_xyz.xlsx
```

**Step 5** At the following prompt, enter your Prime Central administrative username and password:

```
Enter Prime Central admin username:
Enter Prime Central admin user password:
```

The update begins. After update, output similar to the following is displayed:

```
User USER_3 is updated successfully in Prime Central
```

```
User USER_2 is updated successfully in Prime Central
User USER_1 is updated successfully in Prime Central
Number of users requested: 3
Number of users updated: 3
```

- Step 6** Log in to Prime Central and choose **Administration > User and Privilege Management > Users** to open the User Management portlet. Verify that the users you updated are visible in the **Users** tab.
- For the updated users, roles associated to bulk users, their associated groups and relevant domain managers from an Excel file that you create will be updated automatically.

## Retrieving Users in Bulk

From the UNIX command line, you can perform a bulk retrieve of users into an Excel file.

### Procedure

- Step 1** As the *bulkuser* user, log in to the Prime Central server with the *bulkuser* password that you specified during creation.
- Step 2** Change directories to the *installation-directory/utills/prime\_tools/UtilityUsersDir* folder.
- Step 3** Enter the following command to retrieve the users defined in the Prime Central database into the Excel file:

```
sh importUsers -r FILE Excel-filename
```

For example, to update a file named *users\_xyz.xlsx*, enter:

```
sh importUsers-r FILE users_xyz.xlsx
```

**Note** Make sure to enter new an excel file name to retrieve users otherwise, a File already exist message is displayed.

- Step 4** At the following prompt, enter your Prime Central administrative username and password:

```
Enter Prime Central admin username:
Enter Prime Central admin user password:
```

The retrieve begins. After retrieve, output similar to the following is displayed:

```
*** retrieving users ***
Retrieval of users from Prime Central is successfully done.
```

- Step 5** Log in to Prime Central and choose **Administration > User and Privilege Management > Users** to open the User Management portlet. Verify that the users, which are visible in the **Users** tab are retrieved in the Excel file.

## Deleting Users in Bulk

From the UNIX command line, you can perform a bulk delete of users from an Excel file that you create.

### Procedure

---

- Step 1** As the *bulkuser* user, log in to the Prime Central server with the *bulkuser* password that you specified during creation.
- Step 2** Change directories to the *installation-directory/Utils/prime\_tools/UtilityUsersDir* folder.
- Step 3** Create your own Excel file that contains all the users you want to delete; then, add that spreadsheet to the *UtilityUsersDir* folder.

By default, the *UtilityUsersDir* folder contains a sample spreadsheet named *customers.xlsx*. You can structure your Excel file similarly.

The sample *customers.xls* file contains four sheets, each of which corresponds to a step in the User Management portlet > Add wizard.

Each sheet contains a GLOBAL SETTING row with information that will apply to all users, unless you overwrite the global setting with your specified value. If you leave a cell blank, Prime Central uses the global setting.

- Step 4** Enter the following command to delete the users defined in your Excel file into the Prime Central database:

```
sh importUsers-d FILE Excel-filename
```

For example, to delete a file named *users\_xyz.xlsx*, enter:

```
sh importUsers-d FILE users_xyz.xlsx
```

- Step 5** At the following prompt, enter your Prime Central administrative username and password:

```
Enter Prime Central admin username:
Enter Prime Central admin user password:
```

The delete begins. After deletion, output similar to the following is displayed:

```
User USER_3 is deleted successfully from Prime Central
User USER_2 is deleted successfully from Prime Central
User USER_1 is deleted successfully from Prime Central
Number of users requested: 3
Number of users deleted: 3
```

- Step 6** Log in to Prime Central and choose **Administration > User and Privilege Management > Users** to open the User Management portlet. Verify that the users you deleted are not visible in the **Users** tab.
- 

## Reporting User Logins in Bulk

From the UNIX command line, you can run a script to report users who logged in to (or did not log in to) Prime Central within a specific number of days.

### Procedure

---

- Step 1** As the *bulkuser* , log in to the Prime Central portal with the *bulkuser* password that you specified during creation.
- Step 2** Change directories to the *installation-directory/Utils/prime\_tools/UtilityUsersDir* folder.

**Step 3** Enter the following command:

```
sh reportUsers number-of-days {login | notlogin} output-filename
```

For example, to report all users who logged in within the last 10 days and save the data to a text file named `output_abc.txt`, enter:

```
sh reportUsers 10 login output_abc.txt
```

To report all users who did not log in within the last 30 days and save the data to a text file named `output_xyz.txt`, enter:

```
sh reportUsers 30 notlogin output_xyz.txt
```

**Step 4** At the following prompt, enter your Prime Central administrative username and password:

```
Enter Prime Central admin username:  
Enter Prime Central admin user password:
```

The script begins to run. When it finishes, the following output is displayed:

```
Number of users reported: x  
Report is created under filename
```

The output file is saved in the runtime location that you specified; either *absolute-path/filename* or *relative-path/filename*. The output file contains four tab-separated columns that report the username, first name, last name, and last login date and time.

---

## Exporting User Data

Prime Central allows you to export user data to Microsoft Excel. Opening the exported file with any program other than Excel is not recommended.

If you sort or filter the data before exporting it, the exported data is likewise sorted or filtered. If you check the left-most check box for a row, the exported data contains a check box for each checked row.

### Procedure

---

**Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.

**Step 2** In the User Management portlet, click the tab that contains the data you want to export.

**Step 3** Click the **Export to Excel** icon.

**Step 4** At the prompt to open or save the Excel file, click **Open**. The default filename depends on the tab you selected in Step 2.:

- Users tab—`usermgmt-Users-table.xls`
- Groups tab—`usermgmt-Groups-table.xls`
- Roles tab—`usermgmt-Roles-table.xls`
- Privileges tab—`usermgmt-Privileges-table.xls`

**Note** By default, browser caching is enabled. If you disable caching, you might receive the following errors when you try to export user data:

```
Browser cannot download file from server.
Browser was not able to open this Internet site. The requested site is either
unavailable or cannot be found.
Please try again later.
```

**Step 5** Click **Yes** at the following prompt:

```
The file you are trying to open, 'filename', is in a different format than specified by the
file extension.
Verify that the file is not corrupted and is from a trusted source before opening the file.
Do you want to open the file now?
```

## Auditing User Activity

Prime Central collects and stores security audit information, which you can use to track user activity such as logins or logouts, updates of user information, and application cross launches.

### Procedure

**Step 1** From the Prime Central menu, choose **Administration > System > Audit Log**.

The Audit Log portlet opens, displaying user activity for the past 90 days (by default).

**Step 2** To change the default value, do the following:

- a) In the top-right corner of the Audit Log portlet, click the **Options** icon.
- b) Click the **Configuration** link.

The Audit Log - Configuration dialog box opens.

- c) In the Number of Days of Audit Data Retention in Database field, enter the number of days for which you want Prime Central to store user activity. For example, if you enter 10, Prime Central will store activity for the past 10 days.

After the configuration details are saved, the scheduler is triggered periodically to reflect the changes from the next day.

- d) Click **Save**.

## Using an External Authentication Provider (LDAP or AAA Server) for User Authentication

By default, Prime Central uses internal authentication, which means passwords are stored in and verified against the data that is stored in the Prime Central database. You can also use a Lightweight Directory Access Protocol (LDAP) server or AAA server to manage user authentication externally. If you use external authentication, user information is checked against what is stored in the external LDAP or AAA server (instead of the Prime Central database). The external authentication server only stores login and password information;

information pertaining to user roles is stored in the Prime Central database. The same user must exist in both the Prime Central database and the external authentication server.

## Configuring Prime Central to Communicate with an External LDAP Server

When you configure Prime Central for external user authentication via an Lightweight Directory Access Protocol (LDAP) server, you can choose to add another layer of security by enabling the use of SSL encryption. Complete one of the following procedures to configure an LDAP server connection.

### Configuring a Standard LDAP Server Connection

This procedure uses LDAP terminology, such as distinguished name (DN), common name (CN), and domain component (DC). An LDAP distinguished name uniquely identifies a user in the LDAP database, similar to a full filename but in reverse order. CNs and DCs are attributes of the domain name.

#### Procedure

- 
- Step 1** In the User Management portlet, create a new user as described in [Adding a User](#). For example, create a Prime Central user named *test-admin*.
- Step 2** If the test-admin user does not already exist on the LDAP server, use an LDAP application to create the test-admin user.
- Step 3** Reset the test-admin user's LDAP password, ensuring that you enter this same password in Step 4d.
- Step 4** Do the following to enable LDAP authentication on the Prime Central portal:
- As the primeusr user, log in to the Prime Central portal.
  - In the *installation-directory/XMP\_Platform/tomcat-7.0.23/webapps/SSO/WEB-INF/spring-configuration* folder, open the *cas\_xmp\_authentication\_providers.xml* file and do the following:
    - Uncomment the following bean reference line:
 

```
<ref bean="ldapProviderPRIME" />
```
    - If your *ldapUserDn* value is configured to something other than *uid*, replace *uid* with that value in the following line:
 

```
<constructor-arg index="1" value="(uid={0})" />
```
- Note** If your LDAP server makes use of the Windows Active Directory, run the following command to obtain the value you need to specify:
- dsquery user -name test-admin**
- The value you are looking for is the first variable listed in the resulting output. In the following example, *CN* is the correct value.
- ```
"CN=test-admin,CN=Users,DC=t4,DC=local"
```
- Run the following script to encrypt the *ldapPassword* setting:
 

```
# portalAAAEncrypt
```
  - Enter the password (for example, **Cisco123**) that you want to encrypt. The script returns an encrypted value (for example, **zhEaxSqhTpJY0R2vStJJBQ==**) that you can use for the *ldapPassword* setting in the next step.

- e) In the *installation-directory/XMP\_Platform/conf/prime/conf/extprovider.properties* file, configure the LDAP settings. See the [Table 7: Sample LDAP Server Settings](#) for a listing of sample settings.

**Step 5** As the `primeusr` user, enter the following commands to restart the Prime Central portal:

**portactl stop**

**portactl start**

You can now use the external authentication server for Prime Central authentication. In this example, the credentials to log in to the Prime Central portal are:

- Username: `test-admin`
- Password: *test-admin's password as configured on the external authentication server*

### Sample LDAP Server Settings

The following table provides samples of the settings you would specify when configuring an LDAP server for Prime Central authentication.

**Table 7: Sample LDAP Server Settings**

| Setting                     | Sample Value                                         | Description                                                                                                                                                                                                                                                         |
|-----------------------------|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ldapServerName</code> | <code>ldap://209.165.200.254:56425</code>            | LDAP server IP address or hostname and directory server port number.                                                                                                                                                                                                |
| <code>ldapUserDn</code>     | <code>CN=test-admin,CN=Users,DC=t4,DC=local</code>   | LDAP server user ID to log in to the LDAP server.<br><br>To obtain the value you need to specify for this setting, run the following command:<br><br><b>dsquery user -name test-admin</b><br><br><b>Note</b> Exclude the quotation marks when you enter this value. |
| <code>ldapPassword</code>   | (Encrypted)<br><code>zhEaxSqhTpJY0R2vStJJBQ==</code> | LDAP server user password to log in to the LDAP server.                                                                                                                                                                                                             |
| <code>ldapBase</code>       | <code>CN=Users,DC=t4,DC=local</code>                 | LDAP base of LDAP users for authentication.                                                                                                                                                                                                                         |

### Configuring an SSL-Encrypted LDAP Server Connection

#### Procedure

- Step 1** In the User Management portlet, create a new user as described in [Adding a User](#). For example, create a Prime Central user named *test-admin*.
- Step 2** If the `test-admin` user does not already exist on the LDAP server, use an LDAP application to create the `test-admin` user.

- Step 3** Enable SSL encryption on your LDAP server, following the instructions provided in the documentation for your server.
- Step 4** In the first line of the `extprovider.properties` file, which can be found in the `installation-directory/XMP_Platform/conf/prime/conf` folder:
- Replace `ldap:` with `ldaps:`
  - Ensure that the correct SSL port number is referenced
- For example, if port number 10636 is designated for SSL use on your server, the first line of the `extprovider.properties` file should look like this:
- ```
ldapServerName=ldaps://$Your_Server:10636
```
- Step 5** Export the LDAP SSL keystore certification by entering the following command:
- ```
keytool -export -keystore Your_LDAP.ks -alias Your_Domain -file Your_LDAP.cer
```
- This command will create the keystore certificate (in this example, `Your_LDAP.cer`).
- Make sure to specify the same `.ks` file you set up when you enabled SSL encryption on your LDAP server.
- Step 6** Import the keystore certificate into the Prime Central keystore by entering the following command:
- ```
keytool -import -alias Your_Domain -file Your_LDAP.cer -keystore $XMP_Home/jre/lib/security/cacerts
```
- where `XMP_Home` is the Prime Central installation directory.
- Step 7** As the root user, enter the keystore password.
- Step 8** Restart the Prime Central portal.
- Step 9** (Optional) To verify that you have set up the LDAP server connection correctly using an LDAP client, such as `jexplorer`, import the keystone certificate to your local client machine by entering the following command:
- ```
keytool -import -alias Your_Domain -file Your_LDAP.cer -keystore $JAVA_Home/jre/lib/security/cacerts
```
- where `JAVA_Home` is the JDK installation directory.

---

## Configuring Prime Central to Communicate with an External AAA Server

Use this procedure to configure the Prime Central portal to communicate with the AAA (RADIUS or TACACS+) server, and to test the connection after it is configured. This procedure uses AAA terminology. User can configure upto three TACACS+ servers.

### Procedure

---

- Step 1** In the User Management portlet, create a new user as described in [Adding a User](#). For example, create a Prime Central user named `test-admin`.
- Step 2** If the `test-admin` user does not already exist on the AAA server, use an AAA application to create the `test-admin` user.
- Step 3** Do the following to enable AAA authentication on the Prime Central portal:
- a) As the `primeusr`, log in to the Prime Central portal.

- b) In the *installation-directory*/XMP\_Platform/tomcat-7.0.23/webapps/SSO/WEB-INF/spring-configuration folder, open the `cas_xmp_authentication_providers.xml` file and uncomment the following bean reference line:
- For TACACS+, uncomment:
 

```
<ref bean="jaasTacacsAuthenticationProviderPRIME" />
```
  - For RADIUS, uncomment:
 

```
<ref bean="jaasRadiusAuthenticationProviderPRIME" />
```
- c) Run the following script to encrypt the `JaasSecretKey` setting:
- ```
# portalAAAEncrypt
```
- d) Enter the secret key (for example, **Cisco123**) that you want to encrypt. The script returns an encrypted value (for example, `zhEaxSqhTpJY0R2vStJJBQ==`) that you can use for the `JaasSecretKey` setting in the next step.
- e) In the *installation-directory*/XMP\_Platform/conf/prime/conf folder, do one of the following:
- For TACACS+, open the `jaas.config.tacacs` file and configure the TACACS+ settings. See the [Table 8: Sample AAA Server Settings](#) for a listing of sample settings.
  - For RADIUS, open the `jaas.config.radius` file and configure the RADIUS settings. See the [Table 8: Sample AAA Server Settings](#) for a listing of sample settings.

**Step 4** As the `primeusr` user, enter the following commands to restart the Prime Central portal:

```
portalctl stop
```

```
portalctl start
```

**Step 5** You can now use the external authentication server for Prime Central authentication. In this example, the credentials to log in to the Prime Central portal are:

- Username: `test-admin`
- Password: *test-admin's password as configured on the external authentication server*

## Sample AAA Server Settings

The following table provides samples of the settings you would specify when configuring a AAA server for Prime Central authentication.

**Table 8: Sample AAA Server Settings**

| Setting         | Sample Value    | Description                           |
|-----------------|-----------------|---------------------------------------|
| <b>TACACS+</b>  |                 |                                       |
| server          | 209.165.200.254 | TACACS+ server IP address or hostname |
| port            | 49              | TACACS+ server port number            |
| secondaryServer | 209.165.200.253 | TACACS+ server IP address or hostname |

| Setting            | Sample Value   | Description  |
|--------------------|--|--|
| secondaryPort      | 49   | TACACS+ server port number   |
| tertiaryServer     | 209.165.200.254  | TACACS+ server IP address or hostname  |
| tertiaryPort       | 49   | TACACS+ server port number   |
| JaasSecretKey      | (Encrypted)TACACS+ server secret key<br>zhEaxSqhTpJY0R2vStJJBQ== | TACACS+ server secret key  |
| <b>RADIUS</b>      |  |  |
| server             | 209.165.200.254  | RADIUS server IP address or hostname   |
| port               | 1812   | RADIUS server port number  |
| JaasSecretKey      | (Encrypted)<br>zhEaxSqhTpJY0R2vStJJBQ==                          | RADIUS server secret key   |
| authenticationType | PAP  | RADIUS server authentication type<br><br><b>Note</b> Only PAP authenticationType is supported by Radius. |

**Sample TACACS Configuration:**

```
TACACS {
    com.cisco.xmp.jaas.tacacs.TacacsLoginModule required
    debug=true
    JaasSecretKey="tIm+wkEvOaUqdbhWSLf+gA=="
    server="172.168.203.200"
    port="49"
    secondaryServer="172.168.203.197"
    secondaryPort="49";
};
```





# CHAPTER 3

## Monitoring Prime Central and the Applications

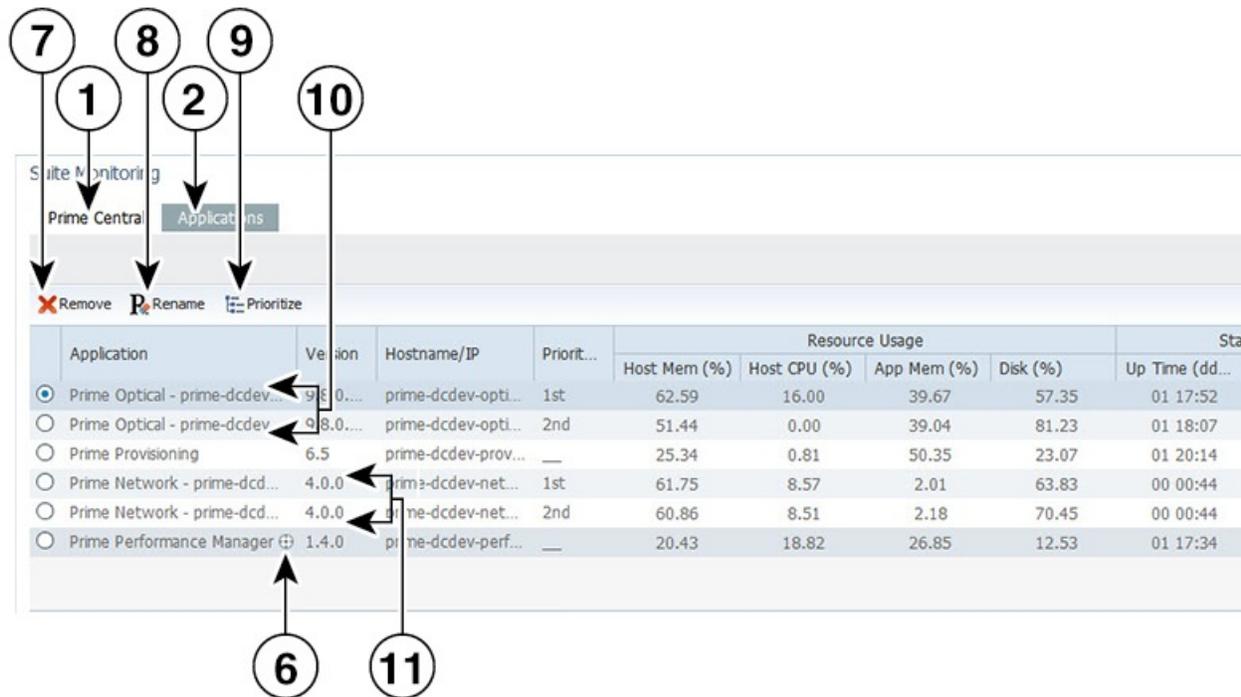
This section describes how to monitor the health status of Prime Central and the individual applications. It contains the following topics:

- [Monitoring the Health of Prime Central and the Applications, on page 57](#)

### Monitoring the Health of Prime Central and the Applications

The following figure shows the Suite Monitoring portlet, where you monitor Prime Central and the individual applications for any changing conditions that might impact operation.

Figure 18: Suite Monitoring Portlet



|   |                   |   |             |
|---|-------------------|---|-------------|
| 1 | Prime Central tab | 7 | Remove icon |
|---|-------------------|---|-------------|

|   |   |    |                                     |
|---|---|----|-------------------------------------|
| 2 | Applications tab                                    | 8  | Rename icon                         |
| 3 | Refresh icon, with last updated time stamp          | 9  | Prioritize icon                     |
| 4 | Settings icon                                       | 10 | Multiple instances of Prime Optical |
| 5 | (When the portlet is maximized) Return to Home icon | 11 | Multiple instances of Prime Network |
| 6 | Quick view icon                                     | —  | —                                   |

## Procedure

**Step 1** From the Prime Central menu, choose **Administration > System > Suite Monitoring**.

**Step 2** In the Suite Monitoring portlet, click the **Prime Central** tab, where you can monitor the information described in the [Table 9: Prime Central and Application Monitoring Information](#).

If multiple Prime Central integration layer profiles are installed, all profiles are shown. For example:

- Integration Layer - Core—The integration layer core components.
- Integration Layer - Messaging—A separate Java Message Service (JMS) broker that enables the integration layer messaging framework to be configured as a JMS cluster for messaging service high availability.

**Step 3** Click the **Applications** tab. For each application, you can monitor the information described in the [Table 9: Prime Central and Application Monitoring Information](#). If multiple instances of Prime Network or Prime Optical are installed, all instances are shown by their service name (not their hostname).

Prime Central supports multiple instances of Prime Network and Prime Optical, for a total of five instances, in any combination. For example:

- Five instances of Prime Network
- Five instances of Prime Optical
- Three instances of Prime Network, plus two instances of Prime Optical (or vice versa)
- Four instances of Prime Optical, plus one instance of Prime Network (or vice versa)

**Note** While Prime Central allows you to monitor more than five instances of Prime Network and Prime Optical, we scale-certified up to only three instances. If you choose to monitor more than five instances, proceed with caution.

**Step 4** To rename multiple instances of Prime Network or Prime Optical:

a) In the Applications tab, select an application instance and click Rename.

You cannot rename an application that has only one instance.

b) Enter the new instance name, which can contain letters (A-Z, a-z), numbers (0-9), and the following special characters: spaces ( ), hyphens (-), underscores (\_), and periods (.).

c) Click **OK**.

## Prime Central and Application Monitoring Information

The following table describes the high-level information you can monitor for Prime Central and the applications running in your network.

**Table 9: Prime Central and Application Monitoring Information**

| Field                | Description   |
|----------------------|---|
| <b>Prime Central</b> |   |
| Component            | Name of the Prime Central component.  |
| Version              | Prime Central version that is running.  |
| Hostname/IP          | Hostname or IP address of the Prime Central portal.   |
| Resource Usage       | <p>Percentage of memory, CPU, and disk space that the application process has used, in terms of preconfigured thresholds. Stable memory consumption reflects a healthy network.</p> <ul style="list-style-type: none"> <li>• If the Prime Central integration layer does not return values, the Resource Usage fields show Not Available.</li> <li>• If the Prime Central integration layer returns invalid values, the Resource Usage fields show Unknown.</li> </ul>  |
| Status               | Number of days, hours, and minutes (in <i>dd:hh:mm</i> format) that the Prime Central component has been running, plus the current state (Up or Down). The Prime Central integration layer shows Up when a ping to it succeeds.   |
| Time Last Checked    | Time stamp when the Prime Central portal was most recently monitored.   |
| <b>Applications</b>  |   |
| Application          | Name of the installed application.  |
| Version              | Version number of the application.  |
| Hostname/IP          | Hostname or IP address of the application.  |
| Priority to Launch   | Priority level of the Prime Network or Prime Optical instance, when multiple instances of the application are installed.  |
| Resource Usage       | <p>Percentage of host memory, host CPU, application memory, and disk space that the application process has used, in terms of preconfigured thresholds.</p> <ul style="list-style-type: none"> <li>• If the application does not return values, the Resource Usage fields show Not Available.</li> <li>• If the application returns invalid values, the Resource Usage fields show Unknown.</li> </ul> <p><b>Note</b> Due to the nature of garbage collection in Java, application memory utilization fluctuates depending on the system load and the timing of the garbage collection. If the application memory utilization continues to increase and never decreases, contact the Cisco Technical Assistance Center.</p> |

| Field             | Description  |
|-------------------|--|
| Status            | Length of time that the application has been running, plus the current state (Up or Down).<br>If the application does not respond to a ping, the State field shows Down.<br><br><b>Note</b> If you are in the process of taking a screenshot of the VM running associated Prime applications (such as Prime Optical) and view the Suite Monitoring portlet, the portlet may momentarily indicate that those applications are down. The Suite Monitoring portlet will update shortly thereafter and reflect that the applications are up and running. |
| Time Last Checked | Time stamp when the application was most recently monitored.   |

## Suite Monitoring Information in the Quick View

In the Suite Monitoring portlet, the quick view displays additional component or application information when the cursor rests over the icon shown in the following figure.

Figure 19: Quick View

The screenshot shows the Suite Monitoring portlet with the 'Applications' tab selected. A table lists several applications, including Prime Optical, Prime Provisioning, Prime Network, and Prime Performance Manager. The Prime Performance Manager application is selected, and a detailed view is displayed over it. This view includes application details such as name, COM-URI, hostname, database name, service name, version, install location, and DB port. It also shows resource usage statistics: Host Mem Usage (20.43%), App Mem Usage (21.43%), Host CPU Usage (0.00%), and Disk Usage (12.53%). Other details include Up Time (01 17:55), Time Last Checked (2013-07-19 22:23:45 GMT), Processors (2), and Status (Up).

| Application                    | Version   | Hostname/IP         | Priorit... | Resource Usage |              |             |          | Status          |       |
|--------------------------------|-----------|---------------------|------------|----------------|--------------|-------------|----------|-----------------|-------|
|                                |           |                     |            | Host Mem (%)   | Host CPU (%) | App Mem (%) | Disk (%) | Up Time (dd...) | State |
| Prime Optical - prime-dcdev... | 9.8.0.... | prime-dcdev-opti... | 1st        | 62.48          | 0.00         | 46.18       | 57.35    | 01 18:13        |       |
| Prime Optical - prime-dcdev... |           |                     |            |                |              |             |          | 01 18:28        |       |
| Prime Provisioning             |           |                     |            |                |              |             |          | 01 20:35        |       |
| Prime Network - prime-dcd...   |           |                     |            |                |              |             |          | 00 00:44        |       |
| Prime Network - prime-dcd...   |           |                     |            |                |              |             |          | 00 00:44        |       |
| Prime Performance Manager      |           |                     |            |                |              |             |          | 01 17:55        |       |

## Prioritizing Application Instances

If multiple instances of Prime Network or Prime Optical are installed, specify which instance has priority for functions such as cross-launching and collecting data. When the instance with the highest priority is down, Prime Central will cross-launch or collect data from the next instance in line.

### Procedure

- Step 1** From the Prime Central menu, choose **Administration > System > Suite Monitoring**.
- Step 2** In the Suite Monitoring portlet, click the **Applications** tab.

**Step 3** Click **Prioritize**.

**Step 4** In the Prioritize window, click the application instance and use the **Move up** and **Move down** arrows to configure the desired priority.

**Step 5** Click **OK**.

The instance priority is displayed in the Applications tab. For example, the Prime Network instance with the highest priority is the instance that cross-launches when you choose **Inventory > Common Inventory > Devices > Device Details via Prime Network**.

---

## Monitoring System Activity

At the bottom of the Prime Central home page, all users can view a tabular listing of bulk system activity. Click the **Message Center** (item 10 in the following figure), which shows bulk system requests that affect applications, including jobs that succeed or fail on the individual applications.

The quick view displays detailed job information when the cursor rests over the icon (item 11) in the following figure.

Figure 20: Message Center

Message Center

Clear

Show Quick Filter

| Status                              | ID | Description          | Time Stamp              | Source       | Creator      |
|-------------------------------------|----|----------------------|-------------------------|--------------|--------------|
| <input type="checkbox"/>            | 1  |                      |                         |              |              |
| <input type="checkbox"/>            | 44 |                      |                         |              |              |
| <input checked="" type="checkbox"/> | 3  |                      |                         |              |              |
| <input type="checkbox"/>            | 4  |                      |                         |              |              |
| <input type="checkbox"/>            | 5  |                      |                         |              |              |
| <input type="checkbox"/>            | 6  |                      |                         |              |              |
| <input type="checkbox"/>            | 7  | DM User Delta Update | 2013-07-18 04:35:22 GMT |              | System       |
| <input type="checkbox"/>            | 8  | COMPOSITE            | 2013-07-18 04:39:06 GMT | centraladmin | centraladmin |
| <input type="checkbox"/>            | 21 | DM User Delta Update | 2013-07-18 14:01:53 GMT |              | System       |
| <input type="checkbox"/>            | 22 | DM User Delta Update | 2013-07-18 14:01:54 GMT |              | System       |
| <input type="checkbox"/>            | 23 | DM User Delta Update | 2013-07-18 14:01:56 GMT |              | System       |
| <input type="checkbox"/>            | 24 | DM User Delta Update | 2013-07-18 14:01:57 GMT |              | System       |
| <input type="checkbox"/>            | 25 | DM User Delta Update | 2013-07-18 14:08:24 GMT |              | System       |
| <input type="checkbox"/>            | 26 | DM User Delta Update | 2013-07-18 14:08:27 GMT |              | System       |
| <input type="checkbox"/>            | 27 | DM User Delta Update | 2013-07-18 14:09:01 GMT |              | System       |
| <input type="checkbox"/>            | 28 | DM User Delta Update | 2013-07-18 14:09:02 GMT |              | System       |
| <input type="checkbox"/>            | 29 | DM User Delta Update | 2013-07-18 14:09:03 GMT |              | System       |
| <input type="checkbox"/>            | 30 | DM User Delta Update | 2013-07-18 14:09:09 GMT |              | System       |
| <input type="checkbox"/>            | 31 | DM User Delta Update | 2013-07-18 14:09:20 GMT |              | System       |
| <input type="checkbox"/>            | 32 | DM User Delta Update | 2013-07-18 14:09:21 GMT |              | System       |
| <input type="checkbox"/>            | 33 | DM User Delta Update | 2013-07-18 14:09:27 GMT |              | System       |
| <input type="checkbox"/>            | 34 | DM User Delta Update | 2013-07-18 14:09:38 GMT |              | System       |

Alarm Summary 1 46 24 19

|   |                               |    |                                     |
|---|-------------------------------|----|-------------------------------------|
| 1 | Number of selected table rows | 7  | Show drop-down list and Filter icon |
| 2 | Total table rows              | 8  | Filter parameters area              |
| 3 | Pull up/pull down toggle icon | 9  | Properties pane                     |
| 4 | Pull out icon                 | 10 | Message Center area                 |

|   |  |    |                 |
|---|--|----|-----------------|
| 5 | Close icon                                 | 11 | Quick view icon |
| 6 | Refresh icon, with last updated time stamp | 12 | Clear icon      |

The following table describes the Message Center information, where:

- Users with administrator-level privileges can see their own bulk job records, plus any system-generated jobs.
- Users without administrator-level privileges can see only their own bulk job records.

**Table 10: Message Center Fields**

| Field       | Description   |
|-------------|---|
| Status      | Whether the job succeeded, failed, or is still pending.   |
| ID          | ID that Prime Central assigns to the bulk job.  |
| Description | Description of the bulk job.<br><br>The following are the four most common operations logged in the Message Center: <ul style="list-style-type: none"> <li>• CREATE—New users have been created in one or multiple Prime Carrier Management applications, such as Prime Network and Prime Optical.</li> <li>• UPDATE—User information has been updated in one or multiple applications.</li> <li>• DELETE—Users have been deleted from one or multiple applications.</li> <li>• COMPOSITE—Indicates a combination of the three previous operations (such as the creation of a new user in Prime Network and the update of a user's information in Prime Optical.</li> </ul> |
| Time Stamp  | Date and time the job was logged.   |
| Source      | Name of the entity on which the bulk job ran; for example, a username for a user management-related job.  |
| Creator     | Name of the user who created the bulk job.  |
| Domain      | Prime Central component or application on which the bulk job occurred.  |

Note the following:

- After using the CLI to import new users into Prime Central 1.5.3 the messages that are normally generated after adding new users are not logged in to the Message Center.
- A user cannot view the messages generated for another user that performed fault or user management operations.
- A `DM User Delta Update` message is logged whenever a Prime Carrier Management application is brought online after being in the Down state previously.
- You are not allowed to clear Message Center items whose status is Pending.

## Monitoring Prime Provisioning Service Requests

Users with the appropriate role can add the following portlets to monitor Prime Provisioning service requests (SRs):

- Device SR Count portlet (Figure 21: Device SR Count Portlet—Most Failed Services and Figure 22: Device SR Count Portlet—Most Successful Services figures)
- SR Summary portlet (Figure 23: SR Summary Portlet figure)

### Procedure

---

- Step 1** On the Prime Central home page, click the **Add Portlets** icon.
  - Step 2** In the Add Portlets dialog box, click **Cisco Prime**.
  - Step 3** Select the following portlets and click **Add**:
  - Step 4** Click the Close (**X**) icon to close the Add Portlets dialog box.
- 

### Device SR Count Portlet

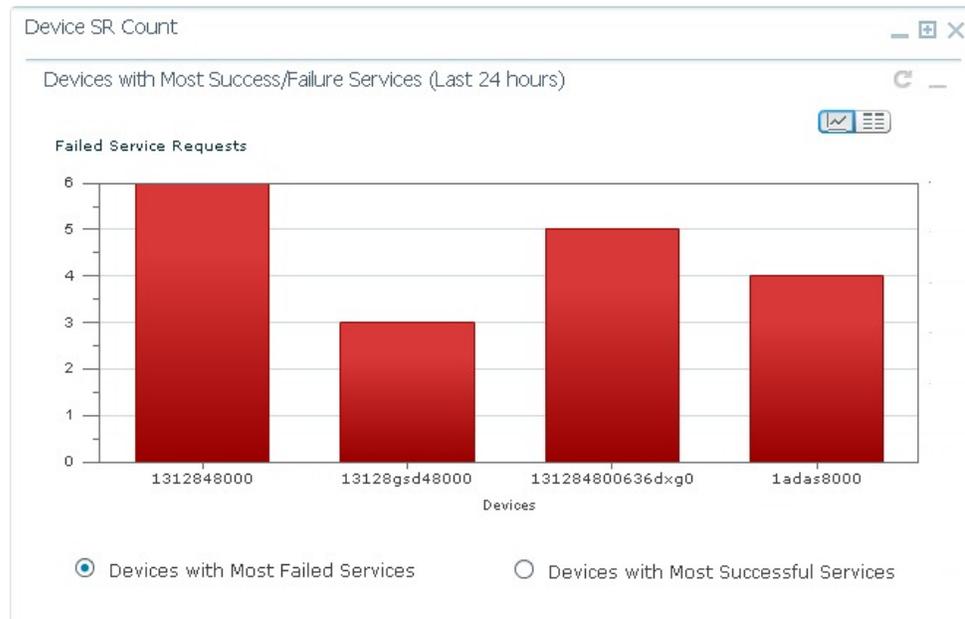
The Device SR Count portlet displays in bar chart format the top 10 devices with the most failed or successful SRs for the last 24 hours. Note that:

- Devices with failed SRs are shown in red (first figure below).
- Devices with successful SRs are shown in blue (second figure below).
- The vertical axis (y-axis) shows the SR count.
- The horizontal axis (x-axis) shows the device name.

You can toggle the display between successful and failed SRs by clicking the radio buttons **Devices with Most Failed Services** and **Devices with Most Successful Services**.

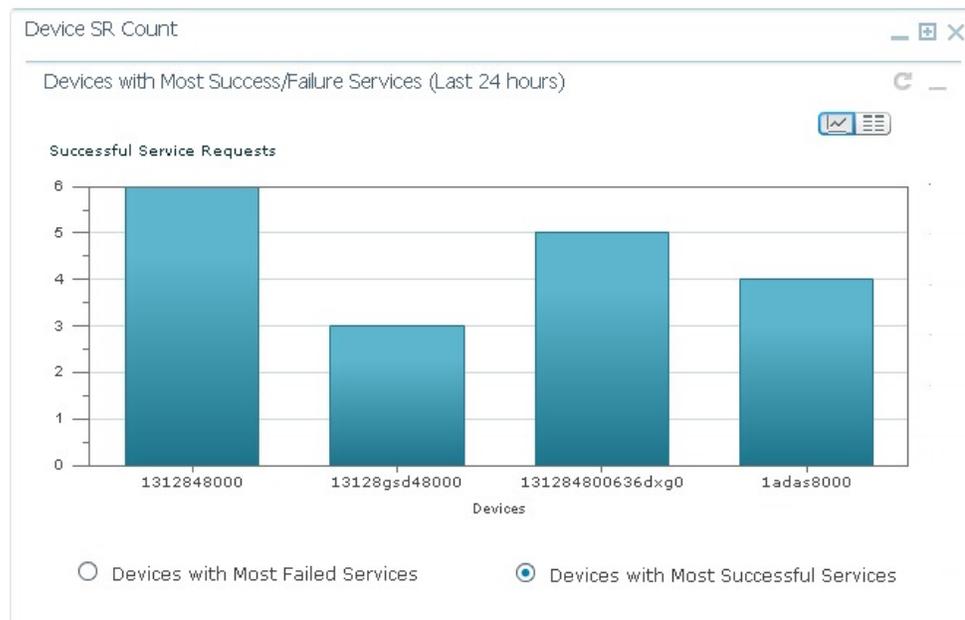
You can view the data in table format by clicking **View as Grid**.

Figure 21: Device SR Count Portlet—Most Failed Services



300264

Figure 22: Device SR Count Portlet—Most Successful Services



300263

## SR Summary Portlet

The SR Summary portlet (see the following figure) provides a count of Prime Provisioning SRs in different states and lists the SRs deployed for the last seven days. The portlet contains the following charts:

- Service Request State pie chart—Displays the number of SRs in different states. SRs are grouped into three main categories:

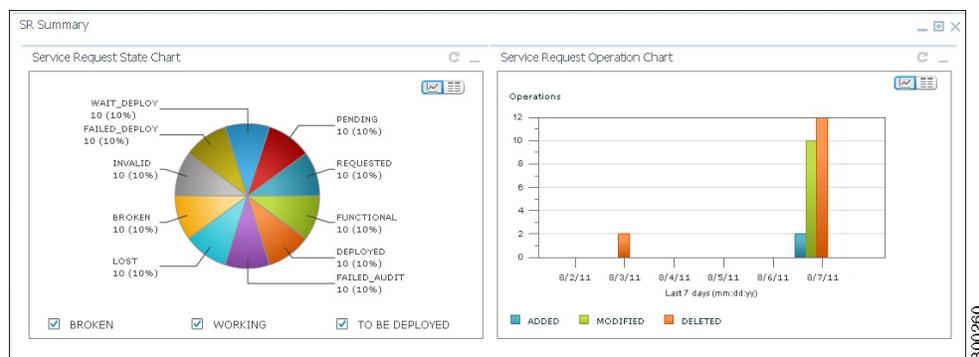
- Broken (includes SRs in FAILED\_DEPLOY, INVALID, BROKEN, LOST, and FAILED\_AUDIT states)
- Working (includes SRs in DEPLOYED and FUNCTIONAL states)
- To be deployed (includes SRs in WAIT\_DEPLOY, REQUESTED and PENDING states)

You can view SRs in different states by checking the BROKEN, WORKING, and TO BE DEPLOYED check boxes.

- Service Request Operation bar chart—Displays the number of SRs that were added, modified, or deleted in the last seven days. The date is displayed in *mm/dd/yy* format.

You can view either chart in table format by clicking **View as Grid**.

**Figure 23: SR Summary Portlet**



## Changing the Prime Central Transport Type Policy

From the UNIX command line, you can configure Prime Central to use SSL or Java New I/O (NIO) as the connection transport type.

The following procedure is optional. Complete it only if you want to change the Prime Central transport type from SSL to NIO (or vice versa) after installation.

### Procedure

- Step 1** As the `primeusr` user, log in to the Prime Central portal with the `primeusr` password that you specified during installation.
- Step 2** Change directories to the `installation-directory/install/scripts` folder.
- Step 3** Enter the following command:  

```
./ilModifyTransportTypeUtil
```
- Step 4** At the following prompts, enter your Prime Central administrative username and password  

```
Enter Prime Central admin username:
Enter Prime Central admin user password:
```
- Step 5** At the following prompt, enter `nio` or `ssl`:  

```
Enter Connection Transport Type [ssl/nio]:
```

For example, to change the transport type to SSL, the script usage is as follows:

```
primeusr@prime-dev-lnx [~/install/scripts]# ./ilModifyTransportTypeUtil
Enter Prime Central admin username:
centraladmin
Enter Prime Central admin user password:
Enter Connection Transport Type [ssl/nio]:
ssl
```

**Note** After the `ilModifyTransportTypeUtil` script is run at least once, the output is available in the `installation-directory/install/logs/ilModifyTransportTypeUtil.log` file.

**Step 6** As the `primeusr` user, log in to the Prime Central portal and enter the following commands to restart it:

```
portalctl stop
portalctl start
```

---

## Removing an Application Manager from the Suite Monitoring Portlet

The following steps remove application information—including the user roles specific to that application—from the Prime Central database.

To completely unregister an application from Prime Central, see "Unregistering an Application from Prime Central" in the [Cisco Prime Central 1.5.3 Quick Start Guide](#).

### Procedure

---

**Step 1** From the Prime Central menu, choose **Administration > System > Suite Monitoring**.

**Step 2** In the Suite Monitoring portlet, click the **Prime Central** or the **Applications** tab.

**Step 3** Click the radio button for the application that you want to remove.

**Step 4** Click **Remove**.

In the Prime Central tab, if a component cannot be removed, the Remove icon is dimmed.

**Step 5** At the confirmation prompt, click **Yes**.

---





## CHAPTER 4

# Managing Inventory

---

This section describes how to use Prime Central to manage inventory. It contains the following topics:

- [What Is Inventory Management?](#), on page 69

## What Is Inventory Management?

Managing inventory involves maintaining a record of all of devices installed in the network to support the provisioning of services. It also includes collecting information about the device name, type, operational status, IP address, and so on.

Inventory management is one of the fundamental network management functions. When forecasting service growth or even attempting to provision a new service, it is necessary to know the current network inventory. Can the existing inventory support the forecast growth or new service requests, or must additional equipment be ordered and installed onsite? Can your hardware support a new software release? You will need to check the type and revision of hardware to determine the answer. Has a recall been issued by the vendor for a certain hardware revision of a board? Are you affected? You will need to check the inventory again.

Prime Central can quickly capture, display, and store an inventory of the devices in your network. Prime Central remains automatically synchronized with changes relating to inventory that might occur in the network. All inventory information is stored in the Prime Central database and is available at any time.

Prime Central provides different levels of inventory reports:

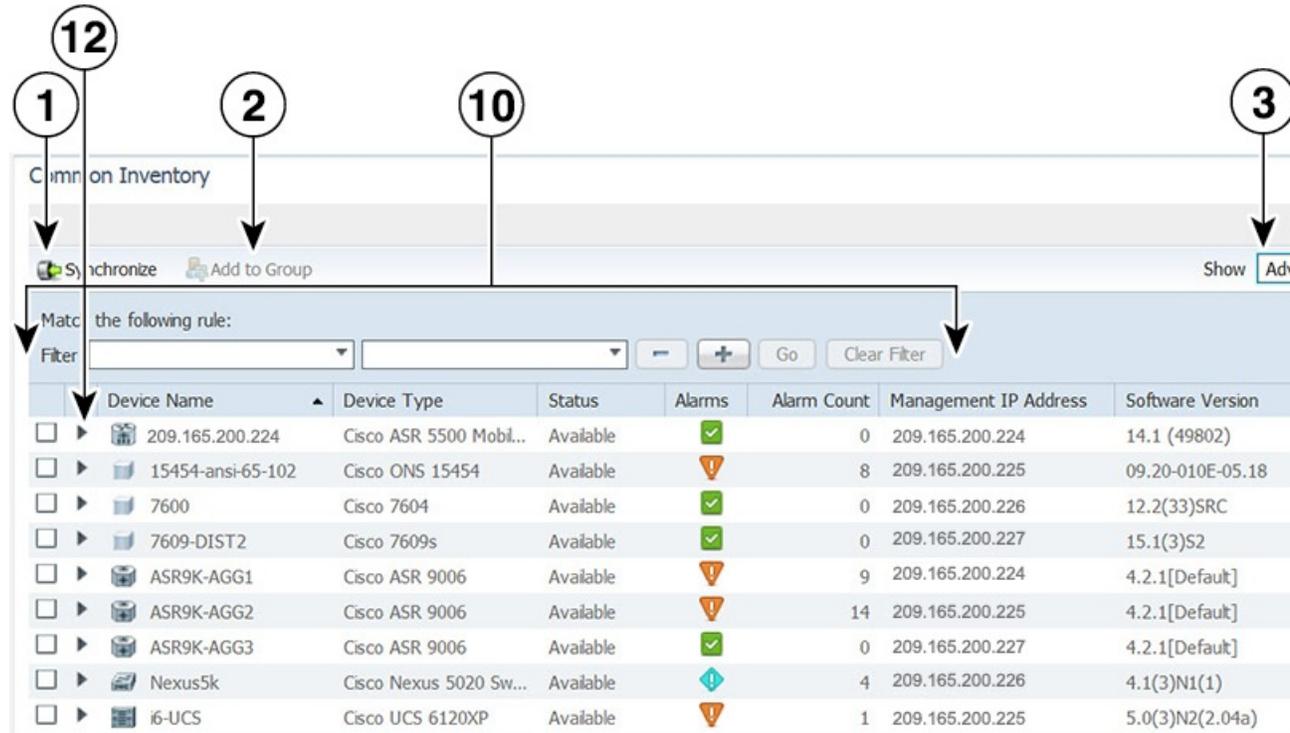
- A complete list of all devices in the network. See [Retrieving Common Inventory Data](#).
- A detailed list of slots, subslots, cards, and modules installed on the devices. See [Retrieving Physical Inventory Data](#).

## Common Inventory Portlet

The following figure shows the Common Inventory portlet, where you can view and manage the devices. Device inventory retrieval involves retrieving device and node information from Prime Network, Prime Optical, and Prime Performance Manager.

The Common Inventory portlet does not display device information for Prime Provisioning.

Figure 24: Common Inventory Portlet



|   |  |    |                        |
|---|--|----|------------------------|
| 1 | Synchronize icon                           | 7  | Export icon            |
| 2 | Add to Group icon                          | 8  | Settings icon          |
| 3 | Show drop-down list                        | 9  | Filter icon            |
| 4 | Number of selected table rows              | 10 | Filter parameters area |
| 5 | Total table rows                           | 11 | Properties pane        |
| 6 | Refresh icon, with last updated time stamp | 12 | Expand icon            |

## Retrieving Common Inventory Data

### Procedure

- Step 1** From the Prime Central menu, choose **Inventory > Common Inventory > Devices**. The Common Inventory portlet opens. For a description of the information provided here, see [Common Inventory Properties Pane](#).

**Note** When an application goes down, its inventory data can get out of sync with the network. To ensure that you are viewing the latest inventory data, we recommended that you perform an on-demand synchronization of user device scopes and inventory. Complete the procedure described in the [Synchronizing Inventory Data](#) topic, selecting the **Synchronize only data received since last synchronization** radio button. We also recommend that you do this after completing the upgrade to Prime Central 1.5.3.

**Step 2** (Optional) Use the Filter icon to view only those devices that are of interest to you. See [Filtering and Searching](#).

## Retrieving Common Inventory Data

### Procedure

**Step 1** From the Prime Central menu, choose **Inventory > Common Inventory > Devices**. The Common Inventory portlet opens. For a description of the information provided here, see [Common Inventory Properties Pane](#).

**Note** When an application goes down, its inventory data can get out of sync with the network. To ensure that you are viewing the latest inventory data, we recommended that you perform an on-demand synchronization of user device scopes and inventory. Complete the procedure described in the [Synchronizing Inventory Data](#) topic, selecting the **Synchronize only data received since last synchronization** radio button. We also recommend that you do this after completing the upgrade to Prime Central 1.5.3.

**Step 2** (Optional) Use the Filter icon to view only those devices that are of interest to you. See [Filtering and Searching](#).

## Common Inventory Properties Pane

The following table describes the information provided in the properties pane of the Common Inventory portlet for the devices in your network.

**Table 11: Common Inventory Properties Pane**

| Field       | Description   |
|-------------|---|
| ID          | Numerical identifier assigned to the device.<br><br>By default, this field is not displayed. For instructions on how to enable it, see <a href="#">Adding or Removing Columns in a Portlet</a> .  |
| Device Name | Icon representing the device, followed by the device name.<br><br>When the same device is managed by multiple instances of Prime Network, the device name must be unique across all the instances of Prime Network.<br><br><b>Note</b> When a device name is changed in Prime Network or Prime Optical, the Common Inventory portlet might show two devices with the new and old names. After ten days, a scheduled job deletes the device with the old name. |

| Field                 | Description   |
|-----------------------|---|
| Device Type           | Type of device.<br><br><b>Note</b> If a CPT device is discovered by both Prime Network and Prime Optical, Prime Optical takes precedence; the Common Inventory portlet reports the physical device details from Prime Optical.  |
| Status                | Communication state of the device: <ul style="list-style-type: none"> <li>• Available—The device is reachable and supported by Prime Central.</li> <li>• Unavailable—Prime Central cannot establish a connection to the device.</li> </ul>  |
| Alarms                | Highest severity alarm on the selected device.<br><br><b>Note</b> To view all alarms on the selected device, click the <b>Expand</b> icon to the left of the device name.   |
| Alarm Count           | Total number of alarms on the selected device.  |
| Management IP Address | IPv4 or IPv6 address of the selected device.<br><br><b>Note</b> The Quick Filter supports a percentage character (%) as a wildcard in the Management IP Address field. Other fields do not use % as a wildcard. To search on complete octets in this field, the % character is not required. Instead, enter a period; the search returns the complete octet after the period. |
| Software Version      | Version of software that is running on the selected device.   |
| System Name           | System name or hostname of the selected device, as defined in the device's MIB.   |
| Vendor                | Device vendor name.   |

## Synchronizing Inventory Data

Administrators can perform an on-demand synchronization of user device scopes and inventory.

### Procedure

- 
- Step 1** From the Prime Central menu, choose **Inventory > Common Inventory > Devices**. The Common Inventory portlet opens.
- Step 2** Click the **Synchronize** icon.
- Note** Only administrators can see the Synchronize icon, which is hidden for all other users.
- Step 3** In the Synchronize dialog box, do the following:
- Click the appropriate radio button:

- **Scopes**—Lets you synchronize device scopes for all Prime Central users. The time stamp of the last synchronization is displayed.
- **Scopes and Inventory**—Lets you synchronize device scopes and inventory. You can synchronize only the data that was received since the last synchronization, or you can synchronize all data. The time stamp of the last synchronization is displayed.

b) Click the **Sync Now** button.

The job status shows “Synchronizing...” until it completes and displays the time stamp of the last synchronization.

**Note** While a device scope synchronization is taking place:

- The **Scopes** radio button is grayed out and not available for selection.
- You can select the **Scopes and Inventory** radio button to synchronize inventory data.

**Step 4** In the Common Inventory portlet, click the **Refresh** icon. The synchronized data is displayed.

**Note** During the sync of large number of devices (for example, more than 5000 devices), inventory may become slow. To overcome this situation, manually perform database optimization tasks called as gatherstats which helps to improve the performance of the inventory sync. This is applicable only when you encounter slowness during inventory sync for the first time. To do gatherstats on database, perform the following:

1. Login as primeusr on linux
2. Navigate to <Install Directory>/install/scripts
3. Run gather\_stats.sh

---

## Retrieving Physical Inventory Data

Physical inventory retrieval involves retrieving information about tangible device and node assets, such as chassis, shelf, module, and port information.

### Procedure

---

**Step 1** From the Prime Central menu, choose **Inventory > Common Inventory > Devices**.

The Common Inventory portlet opens.

**Step 2** To the left of the device name, click the **Expand** icon to view a detailed dashboard for that device (see the following figure).

**Step 3** Expand the chassis to view the physical inventory of the subtending equipment: blades, slots, subslots, cards, and so on.

**Note** When you click a slot, the Common Inventory portlet shows the information described in [Regular Device Attributes for Equipment Holders and Equipment](#).

Figure 25: Device Dashboard Window

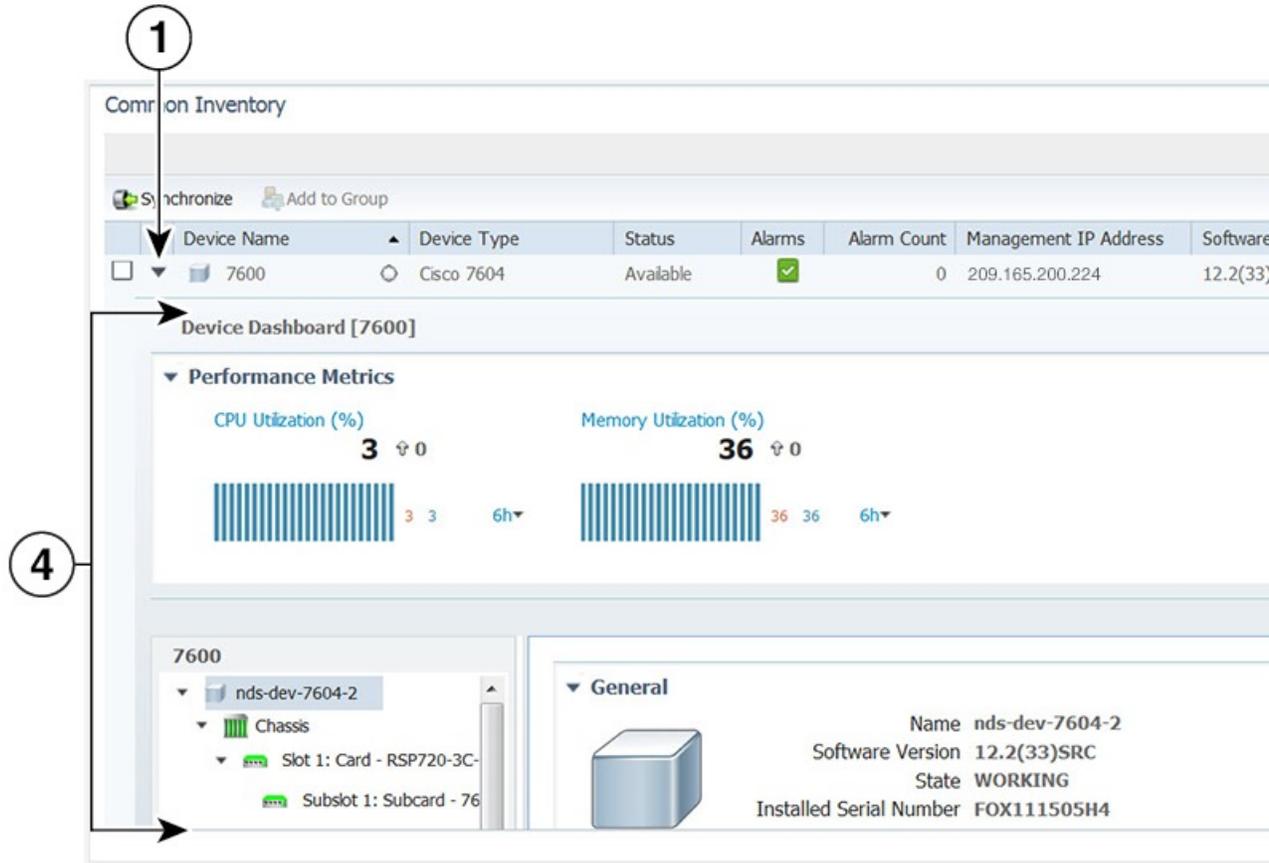


Figure 26: Retrieving Physical Inventory Window

|   |                                    |   |  |
|---|------------------------------------|---|--|
| 1 | Expand icon                        | 3 | Icon to cross-launch Prime Performance Manager |
| 2 | Icon to cross-launch Prime Network | 4 | Device dashboard                               |

## Regular Device Attributes for Equipment Holders and Equipment

The following table lists the regular device attributes for equipment holders and equipment.

| Equipment Holder Attributes | Equipment Attributes    |
|-----------------------------|-------------------------|
| Operational Status          | Description             |
| Hardware Type               | Installed Serial Number |
| Model Type                  | Installed Version       |
| Location                    | Protection Role         |

| Equipment Holder Attributes | Equipment Attributes       |
|-----------------------------|----------------------------|
| —                           | Protection Scheme State    |
| —                           | Resource Fulfillment State |
| —                           | Last Modified Time         |

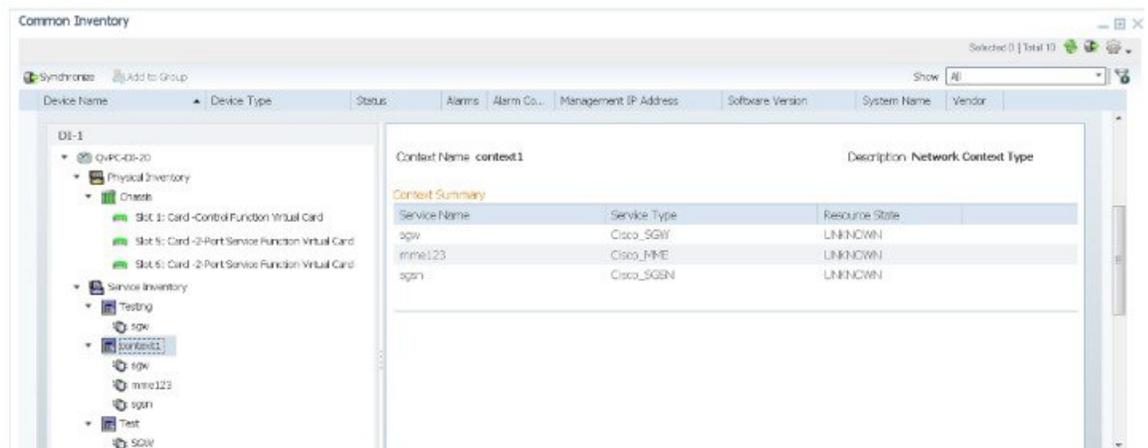
## Retrieving Service Inventory Data

Service Inventory retrieval involves retrieving information on services running on the selected device. All the services in Service Inventory are grouped according to Context.

### Procedure

- Step 1** From the Prime Central menu, choose **Inventory > Common Inventory > Devices**. The Common Inventory portlet opens.
- Step 2** To the left of the device name, click the **Expand** icon to view the detailed dashboard for that device (see the following figure)
- Step 3** In the SI Device panel, click on the required context under **Service Inventory**. The Context information opens in the right side panel with Context Name, Context Description and Context Summary.
- Step 4** In the SI Device panel, expand the required context, to view the services grouped under it.
- Step 5** Click on the required service, to view the inventory details in the right side panel: Service Name, Service Type, Resource State and Last Modified Time.

**Figure 27: Retrieving Service Inventory Data Window**



## Cross-Launching an Application to Retrieve Inventory Details

From Prime Central, you can cross-launch Prime Network, Prime Optical, or Prime Performance Manager and retrieve detailed inventory information. Use the application to retrieve logical inventory information; for example, information about logical resources used for service activation.



### Note

- You can have up to ten cross-launched application windows open simultaneously. You cannot cross-launch an eleventh application until you close one of the open windows.
- You cannot cross-launch Prime Provisioning from anywhere within the Common Inventory portlet.

### Procedure

**Step 1** From the Prime Central menu, choose **Inventory > Common Inventory > Devices**.

The Common Inventory portlet opens.

**Step 2** To the left of the device name, click the **Expand** icon for the desired application.

**Step 3** In the top-right corner of the device dashboard, click the source icon to cross-launch the application. The following table lists the source icons.

If a device is managed by multiple instances of an application, you cross-launch to the instance that has priority (as specified in the Suite Monitoring portlet; see [Prioritizing Application Instances](#)).

*Table 12: Source Icons*

| Click this source icon...   | To cross-launch:          |
|---|---------------------------|
|  | Prime Network             |
|  | Prime Optical             |
|  | Prime Performance Manager |

## Performing a Contextual Cross-Launch to the Data Center Hypervisor Pane

While managing the devices in your network, you can perform a contextual cross-launch to the Data Center's Hypervisor pane and view detailed inventory information for a particular hypervisor.

### Procedure

**Step 1** From the Prime Central menu, choose **Inventory > Common Inventory > Devices**.

The Common Inventory portlet opens.

- Step 2** To the left of the device on which a particular hypervisor resides, click the **Expand** icon to open the corresponding dashboard.
- Step 3** From the object selector pane, click the name of the blade server associated with the hypervisor. The right-hand pane updates, displaying information for that blade server.
- Step 4** From the Equipment section, click the hypervisor's link. The Hypervisor pane (Assure > Data Center > Compute > Hypervisor) opens, displaying detailed inventory information for the selected hypervisor.
- 

## Device Information in the Device 360° View

In the Common Inventory portlet, you can access additional information for a particular device by launching its 360° view . To do so, place your cursor over the device's table entry and then click the radio button in the Device Name column.

The Device 360° view (see the following figure) shows device-specific alarms from the Prime Central Fault Management database, as well as performance charts from Prime Performance Manager.

Click the Alarms or Inventory Summary tabs to see detailed alarm and inventory information. (The features that appear in the Device 360° view differ depending on the device type.)

From the Device 360° view, you can cross-launch the application that manages the device and retrieve detailed inventory information. In the top-right corner, click the source icon listed in the [Table 12: Source Icons](#).

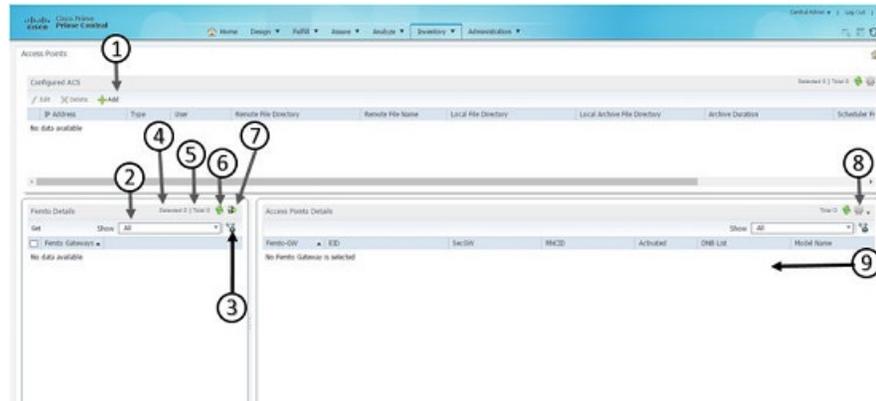
Figure 28: Device 360° View

The screenshot displays the Cisco Prime Central interface. On the left, a 'Common Inventory' list shows various devices, with 'ASR9K-AGG2' selected. The main area shows the 'Device 360° View' for 'ASR9K-AGG2' (IP: 209.165.200.224). Key metrics include CPU Utilization at 6% and Memory Utilization at 70%. Below these are 'Alarms' and 'Inventory Summary' sections, with the latter showing 8 critical/major alarms, including 'Layer 2 tunnel down' and 'Power Supply down'.

## Access Points Portlet

The Access Points portlet in Inventory helps the operator to view access points information in a Femto Gateway service. Access Points provide the capability to amplify network performance, grow revenue, and reduce costs. It combines massive performance and scale with flexibility, virtualization, and intelligence.

Figure 29: Access Points Portlet



|   |   |
|---|---|
| 1 | Configures ACS details panel              |
| 2 | Show drop-down list                       |
| 3 | Filter icon                               |
| 4 | Number of selected table rows             |
| 5 | Total table rows                          |
| 6 | Refresh icon with last updated time stamp |
| 7 | Export icon                               |
| 8 | Settings icon                             |
| 9 | Properties pane                           |

### Access Points Details Panel

The following table describes different field information in Access Point Details panel and other Access Points related information.

**Example:** EID, Femto-GW, Latitude, Longitude, Class of Service, Manufacturer, DNB List.

| Field           | Description   |
|-----------------|---|
| <b>Femto-GW</b> | Used to denote both the HNB gateway and HeNB Gateway that manages different access points.            |
| <b>EID</b>      | Numerical identifier assigned to the Access point.  |
| <b>SecGW</b>    | Used to secure backhaul traffic between the Radio Access Network (RAN) and the operator core network. |
| <b>RNCID</b>    | Radio Network Controller ID. RNC is responsible for controlling the Node BS that are connected to it. |

| Field                       | Description   |
|-----------------------------|---|
| <b>Expected latitude</b>    | Latitude where the Access Point is located.   |
| <b>Expected Longitude</b>   | Longitude where the Access Point is located.  |
| <b>DNB list</b>             | List of the Access Point neighbors.   |
| <b>RF Transmitter State</b> | Displays the state of the RF Transmitter. The state can be either True or False, else 0 or 1.<br><br><b>Note</b> The <b>RF Transmitter State</b> field is available only if the .csv file has the column name as RFTx State. For more information about the csv file format and its configuration information, see <a href="#">Setting up the getDeviceData Cron</a> section. |
| <b>Model Name</b>           | Model of the Access Point.  |
| <b>Software Version</b>     | Version of software that is running on the selected device.   |



**Note** You can add different columns in Access Points portlet, through the **Settings** button at the top right corner.

## Navigating to Access Points Portlet

You can navigate to the **Access Points** portlet in Prime Central through:

- Inventory Menu
- Add Portlet button

### Navigating through Inventory Menu

#### Procedure

- 
- Step 1** From the Prime Central menu, choose **Inventory > Common Inventory > Access Points**. The **Access Points** Portlet appears that displays the following panels:
- **Femto Gateways**: Lists all the Access Points in the Femto Gateway Service
  - **Access Point Details**: Lists Access Points information for the Access Points
- Step 2** From the **Femto Gateways** panel, select the required Femto Gateway or select all.
- Step 3** Click the '>>' button beside the **Show** option and click **Get** button. The Access Point details for the selected Femto Gateway are displayed in the **Access Points Details** panel.
-

## Navigating through Add Portlet button

### Procedure

- Step 1** From the top right corner of the Prime Central portlet, under the **logout** button, click the **Add Portlets** button.
- Step 2** Choose **Cisco Prime > Access Points > Add**.  
The Access Points Portlet opens.

## Configuring Access Points

To view the list of access points available in Access Point portlet, operator should initially provide the configuration details of either RMS/ Spiderweb or Both the servers. You can add, edit or delete RMS or Spiderweb details from the Configured ACS details panel. For more information about the csv file format and its configuration information, see the [Setting up the getDeviceData Cron](#) section.

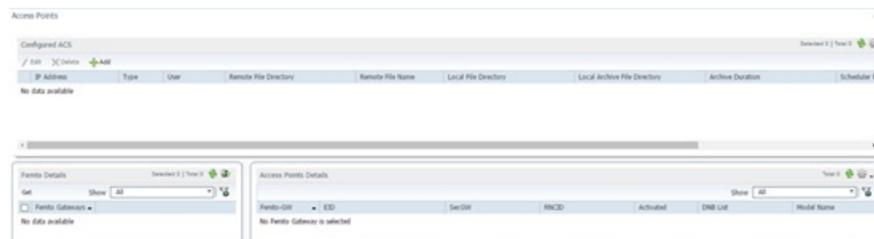


- Note** After saving the configuration from Configuration GUI, the configuration data is stored and scheduler is triggered based on the value of **Scheduler Frequency** time. If Scheduler Frequency time or any other value needs modification, operator needs to update and save the respective configuration fields. The scheduler will be re-triggered at the Scheduled Time.

### Procedure

- Step 1** From the Prime Central menu, choose **Inventory > Common Inventory > Access Points**. The Access Points portlet appears.

*Figure 30: Access Points*



- Step 2** In the **Access Points** Portlet, on the Configured ACS details panel, click **Add** to add RMS and Spiderweb server details. The **Access Points - Configuration** window appears.

Figure 31: Access Points - Configuration

**Access Points - Configuration** X

**Global Scheduler Settings**

Scheduler Frequency (days)

Scheduler Frequency (Time)

**Auto Configuration server**

ACS Type

HOST IP Address

UserID

Password

Remote CSV File Directory

Remote CSV File Name

Local File Directory

Local Archive File Directory

Archive Duration (Days)

Table 13: Global Scheduler Settings

| Fields | Description |
|--------|-------------|
|--------|-------------|

|                            |   |
|----------------------------|---|
| Global Scheduler Settings  | To modify the scheduler settings again check the <b>Global Scheduler Settings</b> check box.<br><br><b>Note</b> Global Scheduler Settings are common for all RMS or Spiderweb configurations, modifying them will affect all configured RMS or Spiderweb details. |
| Scheduler Frequency (days) | Enter the days at which the scheduler frequency is triggered to collect Access Points' data.  |
| Scheduler Frequency (Time) | Enter the time at which the scheduler frequency is triggered to collect Access Points' data.  |

**Table 14: Auto Configuration server**

| Fields                       | Description  |
|------------------------------|--|
| ACS Type                     | From the drop-down list, choose an ACS type for which you want to enter configuration details. The options available are RMS or UCS 8050.<br><br><b>Note</b> For the selected USC 8050 ACS type, you cannot edit the <b>Remote CSV File Directory</b> , <b>Remote CSV File Name</b> , <b>Local File Directory</b> , <b>Local Archive File Directory</b> , and <b>Archive Duration (Days)</b> fields. |
| Host/IP Address              | Enter the IP address of the host.  |
| UserID                       | Enter the User ID of the Spiderweb server or RMS SFTP host.  |
| Password                     | Enter the password for the Spiderweb server or RMS SFTP host.<br><br><b>Note</b> In Prime Central <b>1.5.2</b> , configured Access Control System (ACS) doesn't allow the passwords with a special character "@". You can create passwords of any combination of upper and lowercase characters, numbers, and only special characters that include "!", "#", "\$", "%", "^", "&", "*", "(", and ")". |
| Remote CSV File Directory    | Enter the location of the CSV file on the RMS Server.  |
| Remote CSV File Name         | Enter the name of the CSV file on the RMS Server.  |
| Local File Directory         | Enter the location on the local server where the CSV file is downloaded from the RMS server.   |
| Local Archive File Directory | Enter the location on the local server where the archived CSV file is copied to.   |
| Archive Duration (Days)      | Enter the duration after which the archived CSV file will be deleted.  |

**Step 3** Click **Add** to add the configuration details of the access points.

**Step 4** In the **Access Points** Portlet, to edit the RMS or Spiderweb server detail, select a RMS or Spiderweb server, and then click **Edit**. The **Edit** dialog box appears. Enter new values.

By default, the **Global Scheduler Settings**, **ACS Type** and **Host IP Address** fields will be disabled. To modify the scheduler Settings again, check the **Global Scheduler Settings** check box.

- Step 5** Select a RMS or Spiderweb IP address that you want to delete, and then click **Delete**. Click **Yes** in the Confirmation dialog box to delete the selected RMS or Spiderweb configuration detail. If you want to delete multiple RMS or Spiderweb IP addresses select multiple instances of RMS or Spiderweb IP Addresses, and then click **Delete**.

## Access Points Fault Management

Fault Management helps the operator to view and administrate issues that affect the network. Prime Central raises a BAC alarm when the CSV file download from the RMS server to the local server fails, due to reasons such as file does not exist on the RMS Server, insufficient privileges or invalid file path.

### Procedure

- Step 1** From the Prime Central menu, choose **Assure > Prime Central Fault Management**.
- Step 2** Click **Alarm Browser**.  
The Alarm browser opens that shows the BAC alarms raised while downloading the CSV file from RMS server to the local server.

## Exporting Inventory Data

Prime Central allows you to export inventory data to Microsoft Excel. Opening the exported file with any program other than Excel is not recommended.

If you sort or filter the data before exporting it, the exported data is likewise sorted or filtered.

### Procedure

- Step 1** From the Prime Central menu, choose **Inventory > Common Inventory > Devices**.
- Step 2** In the Common Inventory portlet, click the **Export to Excel** icon.
- Step 3** At the prompt to open or save the Excel file, click **Open**.

**Note** By default, browser caching is enabled. If you disable caching, you might receive the following errors when you try to export inventory data:

"Browser" cannot download file from server.

"Browser" was not able to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later.

- Step 4** Click **Yes** at the following prompt:

The file you are trying to open, "filename", is in a different format than specified by the file extension.

Verify that the file is not corrupted and is from trusted source before opening the file.  
Do you want to open the file now?

---

## Grouping Network Devices and Services

In the Group Management portlet (see the following figure), you can logically group network devices and services by certain criteria. This allows you to organize network elements as you see fit and quickly determine the members of a particular group when necessary.

To view the Group Management portlet, do one of the following:

- Choose **Administration > Group Management > Groups**.
- Add it to the Prime Central home page. See [Adding a Portlet](#) for instructions.

Groups are of two types:

- **User Defined Groups:** This group is further divided into Static and User Defined Dynamic Groups.
  - **Static Groups:** These groups are created under Regions and User Defined-Static Groups. Here the Network Devices are manually populated from Compute, Network, or Storage in the Data Center or from Common Inventory portlet.
  - **User Defined Dynamic Groups:** In this group, the Network Devices are populated into their respective groups based on certain filters given by the user.
- **Prime Central Groups:** They are dynamic groups in which the devices are automatically populated by Prime Central, based on the rules configured for those groups, such as Devices, Storage, Compute Services, and Network Services.

See [Adding a Group Member](#) for more information.

Note the following:

- You cannot manually add members to or delete members from a dynamic group.
- You can only edit or delete user-created groups.
- Of the groups listed in this portlet, you can only create subgroups for the following:
  - Regions
  - User-Defined Static
  - User-Defined Dynamic

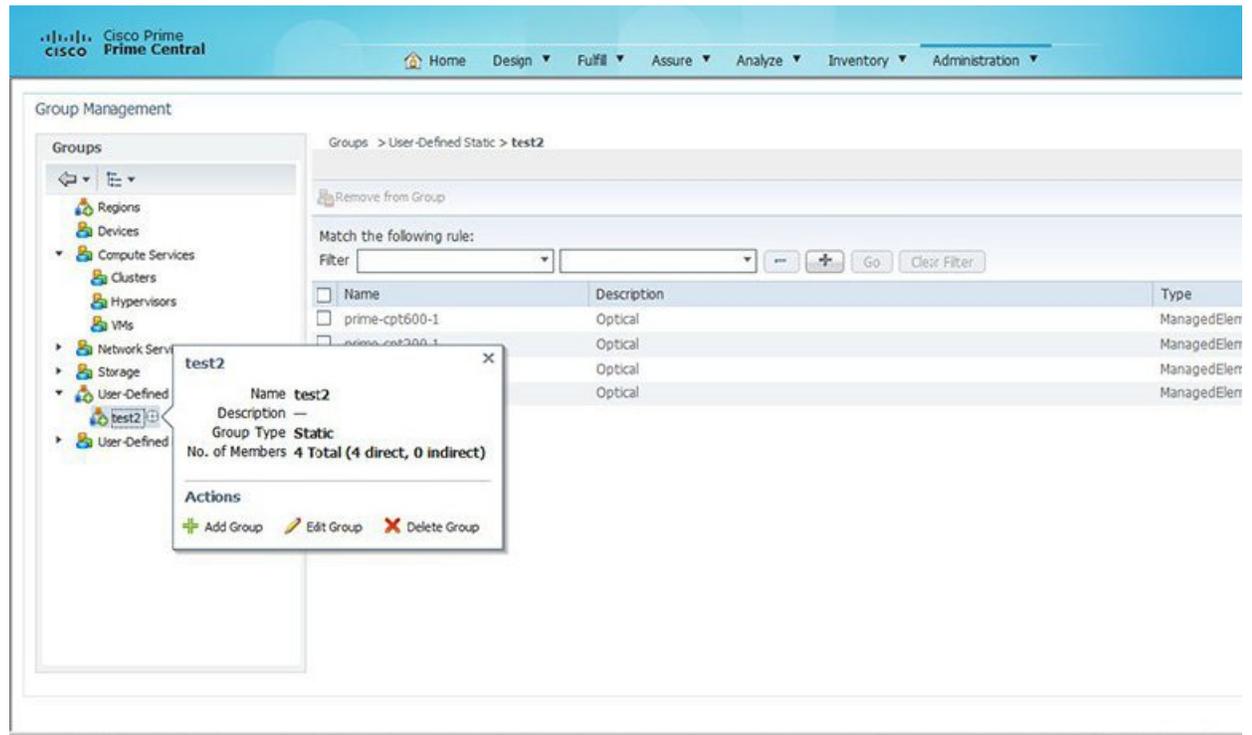


---

**Tip** To view the information in the Group Management portlet as a Microsoft Excel spreadsheet, click the **Export** icon in the top-right corner of the portlet.

---

Figure 32: Group Management Portlet



## Adding a Group

### Procedure

- 
- Step 1** In the Group Management portlet, open the popup for the relevant parent group and click **Add Group**. If this option is not available, you cannot create a group within the selected parent group.
- Step 2** In the Add Group dialog box:
- Enter the group's name, which must contain only alphanumeric characters (A-Z, a-z, 0-9) or any of the following special characters: , - . \_ @
  - Select the appropriate parent group (if necessary).
  - (Optional) Enter a brief description of the group.
 

If you are configuring a dynamic group, proceed to Step 2d. Otherwise, skip ahead to Step 3.
  - Define the rules that Prime Central will use to filter the network elements associated with the group. See [Configuring Group Rules](#) for more information.
- Step 3** Click **Save**.
-

## Configuring Group Rules

When configuring a new dynamic group in the Group Management portlet, you need to specify the rules Prime Central will use to populate the group.

### Procedure

---

- Step 1** In the Group Rules field of the Add Group dialog box, select the object you want to filter by from the second drop-down list.
- Step 2** From the third drop-down list, select the parameter you want to filter by.  
The values listed here will vary, depending on the object you selected in Step 1.
- Step 3** From the fourth drop-down list, select a logical operator.
- Step 4** In the text field, enter the value you want to filter by. This value must contain only alphanumeric characters (A-Z, a-z, 0-9) or any of the following special characters: , - . \_ @  
If you want to configure another rule, proceed to Step 5. Otherwise, skip ahead to Step 8.
- Step 5** Click the + icon.
- Step 6** In the first drop-down list, select whether network elements must meet the conditions of this and any other rules you configured in order to be added to a group.
- Step 7** Repeat Steps 1 through 4.
- Step 8** Click **Save**.
- 

## Editing a Group

### Procedure

---

- Step 1** In the Group Management portlet, open the popup for the relevant group and click **Edit Group**.  
If this option is not available, you cannot edit the selected group.
- Step 2** In the Edit Group dialog box, modify the group's name and description.  
The group's name must contain only alphanumeric characters (A-Z, a-z, 0-9) or any of the following special characters: , - . \_ @
- Step 3** Click **Save**.
- 

## Deleting a Group

### Procedure

---

- Step 1** In the Group Management portlet, open the popup for the relevant group and click **Delete Group**.  
If this option is not available, you cannot delete the selected group.

**Step 2** Click **Yes** to confirm deletion of the group.

---

## Adding a Group Member

### Procedure

---

- Step 1** Do one of the following:
- To add a group member from the Common Inventory portlet, choose **Inventory > Common Inventory > Devices** from the Prime Central menu and skip ahead to Step 3.
  - To add a group member from the Data Center page, choose **Assure > Services > Data Center** from the Prime Central menu and proceed to Step 2.
- Step 2** Do one of the following:
- To add a compute service resource, hypervisor, or device cluster, click the **Compute** tab and then click the appropriate subtab.
  - To add a VPN, click the **Network** tab.
  - To add a storage device, click the **Storage** tab.
- Step 3** Check the check box for the device or service that you want to add and click **Add to Group**.
- Step 4** In the Select Group to Add window, select the appropriate group and click **Add**.  
A message indicates that the member was successfully added.
- Step 5** In the Group Management portlet, click the **Refresh** icon.  
The new group member is displayed.
- 

## Removing a Group Member

### Procedure

---

- Step 1** In the Group Management portlet, navigate to the appropriate group.
- Step 2** Check the check box for the group member that you want to remove and click **Remove from Group**.
- Step 3** Click **Yes** to confirm deletion of the group member.
- 

## Monitoring Alarm Counts for Grouped Devices

In Alarms Count Summary portlet (see the following figure), you can view total count of alarms for each group defined in Group Management portlet. This enables you to have a consolidated view of total number of faults with their highest severity on network elements of a particular group. To view Alarms Count Summary portlet, add it to the Prime Central home page. See [Adding a Portlet](#) for more information on adding a portlet.

In Alarms Count Summary portlet, all User Defined sub-groups are defined in the same level unlike the tree structure in Group Management portlet to enable quick filtering of all subgroups.

You can add devices to User Defined Static Groups manually from Compute, Network, or Storage in the Data Center or from Common Inventory portlet. See [Adding a Group Member](#) for more information on adding members to groups. Once the devices are added to a group, their corresponding alarms count along with their highest severity is displayed in the portlet. Alarms Count Summary portlet will update automatically after every 25 seconds, or click refresh button to update the results in the portlet.

**Figure 33: Alarms Count Summary**

| Groups     | Highest Severity | Alarm Count | Group Name           |
|------------|------------------|-------------|----------------------|
| Regions    | ●                | 8           |                      |
| Devices    | ●                | 11          |                      |
| uds-chk01  | ■                | 0           | User-Defined Static  |
| uds-chk02  | ■                | 0           | User-Defined Static  |
| chk0-2     | ■                | 0           | User-Defined Static  |
| chk0-2-3   | ■                | 0           | User-Defined Static  |
| chk0-2-3-4 | ■                | 3           | User-Defined Static  |
| udd-chk01  | ■                | 0           | User-Defined Dynamic |
| udd-chk02  | ■                | 0           | User-Defined Dynamic |

2015-07-15 11:50:00 GMT

4015432





# CHAPTER 5

## Managing Customers

This section describes how to manage customers in Prime Central and associate them with compute, network, and device resources.

As a network administrator, you can create and manage customers for your assurance solution. You can associate physical and virtual devices and network services with a customer, and assess the impact that network-generated alarms and events have on that customer.

This section contains the following topics:

- [Customer Management Portlet, on page 91](#)

## Customer Management Portlet

The following figure shows the Customer Management portlet, where you perform all customer management tasks.

**Figure 34: Customer Management Portlet**



|   |                               |    |                       |
|---|-------------------------------|----|-----------------------|
| 1 | Number of selected table rows | 9  | Properties pane       |
| 2 | Total table rows              | 10 | Enable icon           |
| 3 | Refresh icon                  | 11 | Disable icon          |
| 4 | Export icon                   | 12 | Remove Resources icon |
| 5 | Settings icon                 | 13 | Add icon              |

|   |                                   |    |             |
|---|-----------------------------------|----|-------------|
| 6 | Show drop-down list               | 14 | Delete icon |
| 7 | Filter icon                       | 15 | Edit icon   |
| 8 | Icon to launch Customer 360° view | —  | —           |

## Managing Customers

You can add, edit, and delete customers; associate customers with resources monitored in the Data Center page; disable and enable customer accounts; and export customer data.

### Adding a Customer

#### Procedure

- 
- Step 1** From the Prime Central menu, choose **Administration > Customer Management > Customers**.
- Step 2** In the Customer Management portlet, click **Add**.
- Step 3** In the **Add Customer** window, enter general information about the new customer, including name (required), industry, contact information, and website URL. The variables that you define must adhere to the constraints described in [Customer Information Constraints](#).
- Step 4** (Optional) Add a customer logo image:
- Click **Add Photo**.
  - Click **Choose File**.
  - Navigate to the desired logo and click **Open**. The logo can have a maximum size of 128 x 128 pixels and 60 KB. Supported file types are .png, .jpg, and .jpeg.
- Step 5** Click **Add**.

The new customer is displayed in the Customer Management portlet.

**Note** Newly added customers are enabled by default.

---

### Customer Information Constraints

When adding or editing a customer, the variables that you define must adhere to the constraints listed in the following table.

Table 15: Customer Information Constraints

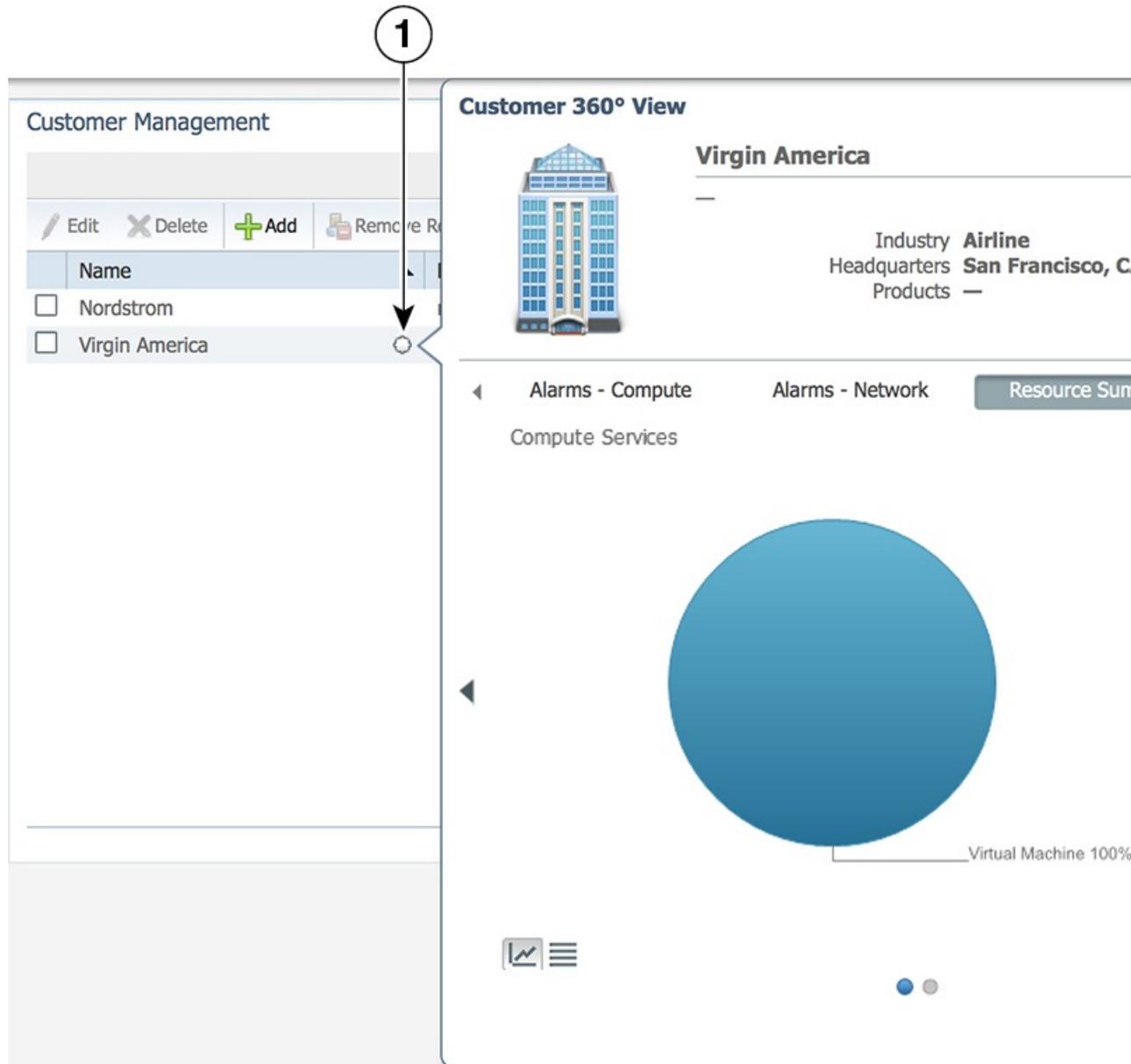
| Variable     | Constraints  |
|--------------|--|
| Name         | The name must: <ul style="list-style-type: none"> <li>• Start with a letter (A-Z, a-z) or a number (0-9).</li> <li>• Contain from 1 to 50 case-sensitive letters (A-Z, a-z), numbers (0-9), hyphens (-), underscores (_), or spaces.</li> <li>• Not contain any other special characters.</li> </ul> |
| Description  | Can contain up to 4000 characters. All characters are allowed.   |
| Industry     | Can contain up to 255 characters. All characters are allowed.  |
| Headquarters | Can contain up to 255 characters. All characters are allowed.  |
| Products     | Can contain up to 2000 characters. All characters are allowed.   |
| URL          | Can contain up to 255 characters. All characters are allowed.  |
| Stock Symbol | Can contain up to 255 characters. All characters are allowed.  |
| Main Contact | Can contain up to 255 characters. All characters are allowed.  |
| Email        | Can contain up to 255 characters. All characters are allowed.  |
| Phone        | Can contain up to 255 characters. All characters are allowed.  |
| Note         | Can contain up to 2000 characters. All characters are allowed.   |
| Photo        | Must be in .png, .jpg, or .jpeg format. The logo cannot exceed 128 x 128 pixels or 60 KB.  |

## Customer Information in the Customer 360° View

In the Customer Management portlet, you can access additional information for a particular customer by launching that customer's 360° view. To do so, place your cursor over the customer's table entry and then click the radio button in the Name column. Click the following tabs within the Customer 360° view:

- Alarms—Shows customer-specific alarms from the Prime Central Fault Management database.
- Resource Summary—Shows the compute, network, or device resources that are associated with the selected customer.
- Contact Info—Shows detailed customer contact information.

Figure 35: Customer 360° View



## Editing a Customer

### Procedure

- Step 1** From the Prime Central menu, choose **Administration > Customer Management > Customers**.
- Step 2** In the Customer Management portlet, select the customer that you want to edit and click **Edit**.
- Step 3** In the Edit Customer window, edit the customer's general information, as required. The variables that you define must adhere to the constraints described in [Customer Information Constraints](#).

- Step 4** Click **Save**.  
The updated customer is displayed in the Customer Management portlet.
- 

## Deleting a Customer

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > Customer Management > Customers**.  
**Step 2** In the Customer Management portlet, select the customer that you want to delete and click **Delete**.  
**Step 3** At the confirmation prompt, click **Yes**.
- 

## Associating Resources to Customers

You can associate resources—virtual machines, bare metal blades, and network services—to customers. A single customer can be associated with multiple resources.

### Procedure

---

- Step 1** From the Prime Central menu, choose **Assure > Services > Data Center**.  
**Step 2** In the Data Center portlet, depending on the type of resource you want to associate, click the **Compute** or **Network** tab.  
**Step 3** Select the desired resource and click **Associate to Customer**.

**Note** You cannot assign the same VPN to multiple customers.

- Step 4** In the **Select Customer to Associate** window, select the desired customer and click **Associate**.

The resource is assigned to the selected customer.

- The Data Center portlet > Customers column shows the name of the customer that is associated with the selected resource. (See first image below.)
- The Customer Management portlet > Resources column shows a green check mark in the row for the selected customer. (See second image below.)

Figure 36: Name of Customer Associated with the Selected Resource

The screenshot shows the Cisco Prime Central interface. The top navigation bar includes Home, Design, Fulfill, Assure, and Analyze. The main content area is titled 'Data Center' and has tabs for Overview, Compute, Network, and Storage. Under the 'Compute' tab, there are sub-tabs for Compute Service, Hypervisor, and Cluster. Below these are action buttons: Synchronize, Set Lifecycle and Priority, Add to Group, and Associate to Customer. A table lists various compute services with the following columns: Name, Status, Alarm, Total Alarm Count, and Server.

|                          | Name                | Status     | Alarm | Total Alarm Count | Server                  |
|--------------------------|---------------------|------------|-------|-------------------|-------------------------|
| <input type="checkbox"/> | Prime-R10-32GB-RHEL | Powered On | ✓     | 0                 | sjo-i6-svr-27.cisco.com |
| <input type="checkbox"/> | Prime-R12-8GB-RHEL  | Powered On | ✓     | 0                 | sjo-i6-svr-27.cisco.com |
| <input type="checkbox"/> | PC-Dev3-8GB-80GB    | Powered On | ✓     | 0                 | sjo-i6-svr-28.cisco.com |
| <input type="checkbox"/> | PC-Dev4-8GB-80GB    | Powered On | ✓     | 0                 | sjo-i6-svr-28.cisco.com |
| <input type="checkbox"/> | PC-Dev5-32GB-100GB  | Powered On | ✓     | 0                 | sjo-i6-svr-28.cisco.com |
| <input type="checkbox"/> | PC-Dev6-32GB-200GB  | Powered On | ✓     | 0                 | sjo-i6-svr-28.cisco.com |
| <input type="checkbox"/> | PC-Dev7-16GB-100GB  | Powered On | ✓     | 0                 | sjo-i6-svr-28.cisco.com |
| <input type="checkbox"/> | PC-Dev8-16GB-100GB  | Powered On | ✓     | 0                 | sjo-i6-svr-28.cisco.com |
| <input type="checkbox"/> | PC-Dev9-16GB-100GB  | Powered On | ✓     | 0                 | sjo-i6-svr-28.cisco.com |
| <input type="checkbox"/> | PC-Dev10-16GB-100GB | Powered On | ✓     | 0                 | sjo-i6-svr-28.cisco.com |
| <input type="checkbox"/> | PC-Dev11-16GB-100GB | Powered On | ✓     | 0                 | sjo-i6-svr-28.cisco.com |

Figure 37: Visual Indication of an Assigned Resource

The screenshot shows the Cisco Prime Central interface. The top navigation bar includes Home, Design, Fulfill, Assure, Analyze, Inventory, and Admin. The main content area is titled 'Customer Management'. Below the title are action buttons: Edit, Delete, Add, Remove Resources, Disable, and Enable. A table lists customers with the following columns: Name, Description, and Industry.

| Name  | Description            | Industry |
|---|------------------------|----------|
| <input checked="" type="checkbox"/> Nordstrom | regional site          | Retail   |
| <input type="checkbox"/> Virgin America       | west coast data center | Airline  |

## Removing Resources from Customers

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > Customer Management > Customers**.
- Step 2** In the Customer Management portlet, select the desired customer and click **Remove Resources**.
- Note** If the selected customer has no resources assigned, the Remove Resources icon is dimmed.
- Step 3** In the **Remove Resources** window, check the check box of the resource that you want to remove; then, click **Remove**.
- The resource is removed from the customer.
- 

## Exporting Customer Data

Prime Central lets you export customer data to Microsoft Excel. Opening the exported file with any program other than Excel is not recommended.

If you sort or filter the data before exporting it, the exported data is likewise sorted or filtered. Each row in the exported data has a check box. If you check the left-most check box for a row before export, the corresponding check box in the exported data is also checked.

To export customer data to an Excel file:

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > Customer Management > Customers**.
- Step 2** In the Customer Management portlet, click the **Export** icon.
- Step 3** At the prompt to open or save the Excel file, click **Open**.
- Note** By default, browser caching is enabled. If you disable caching, you might receive the following errors when you try to export customer data:
- ```
Browser cannot download file from server.  
Browser was not able to open this Internet site. The requested site is either  
unavailable or cannot be found.  
Please try again later.
```
- Step 4** Click **Yes** at the following prompt:
- ```
The file you are trying to open, 'filename', is in a different format than specified by the  
file extension.  
Verify that the file is not corrupted and is from a trusted source before opening the file.  
Do you want to open the file now?
```
-





## CHAPTER 6

# Managing Faults

This section describes how Prime Central locates, diagnoses, and reports network problems.



**Note** Prime Central Fault Management uses a very limited version of the IBM Tivoli Netcool/OMNIBus technology. Some of the windows in the Alarm Browser and Alarm Report portlets have a Help button that launches the IBM Tivoli Netcool online help. See the Cisco license agreement for the limitations that apply.

This section contains the following topics:

- [What Is Fault Management?, on page 99](#)

## What Is Fault Management?

Fault management is the process of locating, diagnosing, and reporting network problems. This is important for increasing network reliability and effectiveness, and for increasing the productivity of network users. Fault management is more than just handling emergencies. It provides functions for managing problems with services and handling customer-facing service problems.

Efficient fault management can:

- Save repair costs through efficient fault detection, location, and correction
- Improve customer care through efficient trouble administration
- Improve service availability and equipment reliability through proactive maintenance and through measurement, review, and corrective action

One responsibility of fault management is to detect faults. A piece of equipment, a transmission medium, a software module, or a database is said to be in a fault state if it cannot perform its intended function and meet all of the requirements placed on that function. The onset of a fault is called a *failure event* and is usually signaled by one or more alarm reports. The termination of a fault state is called a *clear event*.

Fault management is responsible for determining, from a variety of information sources, the root cause of a fault, and for its repair. In certain cases, the root cause of a fault might be in a connecting network. In such cases, fault management is responsible for reporting the problem through appropriate channels.

The steps for successful fault management are:

1. Identify a problem by gathering data about the state of the network (polling and trap generation).

2. Restore any services that have been lost.
3. Isolate the cause, and decide if the fault should be managed.
4. Correct the fault.

## Fault Management Terminology

In Prime Network, an *alarm* represents a scenario that involves a fault in the network, a managed element, or the management system. A *ticket* represents an attention-worthy root cause alarm. A ticket has the same type as the root cause alarm it represents, and it has a status, which represents the entire correlation tree.

In Prime Optical, an *alarm* represents a notification from a managed network element (NE) that a certain fault condition occurred. Alarms usually represent error conditions on NEs. Prime Optical does not use the term *tickets*. NEs managed by Prime Optical perform correlation and suppression and report only root cause alarms.

A *ticket* in Prime Network represents the same information as an *alarm* in Prime Optical.

Prime Central Fault Management uses the term *alarm* to mean a root cause fault condition on which the entire fault lifecycle can be performed.

## Alarm Processing

Prime Network receives events (syslogs and traps) from network elements and performs the first level of alarm correlation. Prime Central Fault Management receives correlated alarms from Prime Network and alarms for Prime Optical and performs second-level, cross-domain alarm correlation and deduplication. Prime Central Fault Management provides an aggregated view of correlated and deduplicated alarms to network operation center (NOC) operators.




---

**Note** Prime Central Fault Management does not retrieve alarm data for Prime Provisioning or Cisco InTracer.

---

Prime Central Fault Management:

- Receives alarms from Prime Optical and tickets from Prime Network.
- Receives system alarms and threshold crossing alerts from Prime Performance Manager.
- Normalizes the alarms and tickets to a common alarm representation to perform aggregation, deduplication, correlation, and enrichment.
- Maintains all active alarms in the Fault Management database. The alarms are also copied from the Fault Management database to the Oracle database for archiving and historical reporting.

## Alarm Aggregation

Alarm aggregation involves the following functions:

- Receive alarms from Prime Optical—Java and CORBA probes use the CORBA northbound interface (NBI) to get and register for alarms from Prime Optical.
- Receive tickets from Prime Network—SNMP probes use the trap forwarding interface to receive tickets, ticket updates, and ticket severity updates from Prime Network.

- Use the Fault Management SNMP probe and the Prime Performance Manager trap forwarding interface to aggregate Prime Performance Manager alarms.
- Normalize and persist received alarms—Probes perform normalization; the Fault Management component persists normalized alarms.

## Alarm Deduplication

Prime Optical and Prime Network manage the same CPT devices and generate the same alarm conditions for CPT managed objects. The following table shows some of the alarm conditions that Prime Optical and Prime Network generate for the same managed objects, and for which Prime Central Fault Management performs deduplication.

**Table 16: Deduplication of Alarm Conditions**

| Prime Optical Alarm Condition                        | Prime Network Alarm Condition    |
|--|----------------------------------|
| Equipment failure                                    | Card down                        |
| Equipment unplugged, missing, or removed incorrectly | Card out                         |
| AIS, LOS, LOF on port                                | Port/link operational/admin down |

The following example illustrates an alarm deduplication:

### Prime Optical Alarm

- Probable Cause—LOS.
- Object Name—ONS-SJC/rack=1/shelf=1/slot=3/port=4.
- Node—209.165.202.129.

### Prime Network Alarm

- cenAlarmDescription—Port Down Due to Admin.
- cenAlarmManagedObjectClass—{[ManagedElement(Key=ONS-SJC)][PhysicalRoot][Chassis][Shelf(ShelfNum=1)][Slot(SlotNum=3)][Module][Port(PortNumber=TenGigabitEthernet1/3/4)][PhysicalLayer]}.
- cenAlarmManagedObjectAddress—209.165.202.129.

## Alarm Correlation

Prime Central Fault Management correlates Layer 2 or Layer 3 alarms generated by Prime Network to the root cause that Prime Optical detects in the dense wavelength-division multiplexing (DWDM) optical layer. In Prime Central 1.5.2, cross-application correlation is limited to within the same CPT, meaning the root cause alarm and the correlated alarm are on the same CPT device.

Prime Central Fault Management performs correlation of the alarm conditions listed in the following table by Prime Optical and Prime Network.

Table 17: Alarm Correlation

| Prime Optical Alarm     |                                    | Prime Network Alarm |                            |
|-------------------------|------------------------------------|---------------------|----------------------------|
| Probable Cause          | Object Name/ Location              | cenAlarmDescription | cenAlarmManagedObjectClass |
| FEC-MISM, OTUK-TIM, LOM | MPLS-TP enabled uplink port on CPT | MPLS-TP LSP down    | OID of MPLS-TP LSP         |

## Alarm Aging

Prime Central Fault Management uses the following alarm aging policy:

- By default, cleared alarms are deleted from the Prime Central Fault Management database after 60 minutes.
- Indeterminate and informational alarms that are not being used for service impact analysis or customer impact analysis are deleted after 1 day.
- Warning alarms that are not being used for service impact analysis or customer impact analysis are deleted after 7 days.
- Active alarms that do not meet the preceding criteria persist indefinitely in the database, unless a user clears them manually.
- The Prime Central database mirrors and archives the Prime Central Fault Management database. When you delete an alarm from the Prime Central Fault Management database, it is deleted immediately. However, the Prime Central database retains the deleted alarm for 14 days, and then purges it.




---

**Note** User can configure alarm retention period, to configure please refer [Configuring Alarms Retention Period](#).

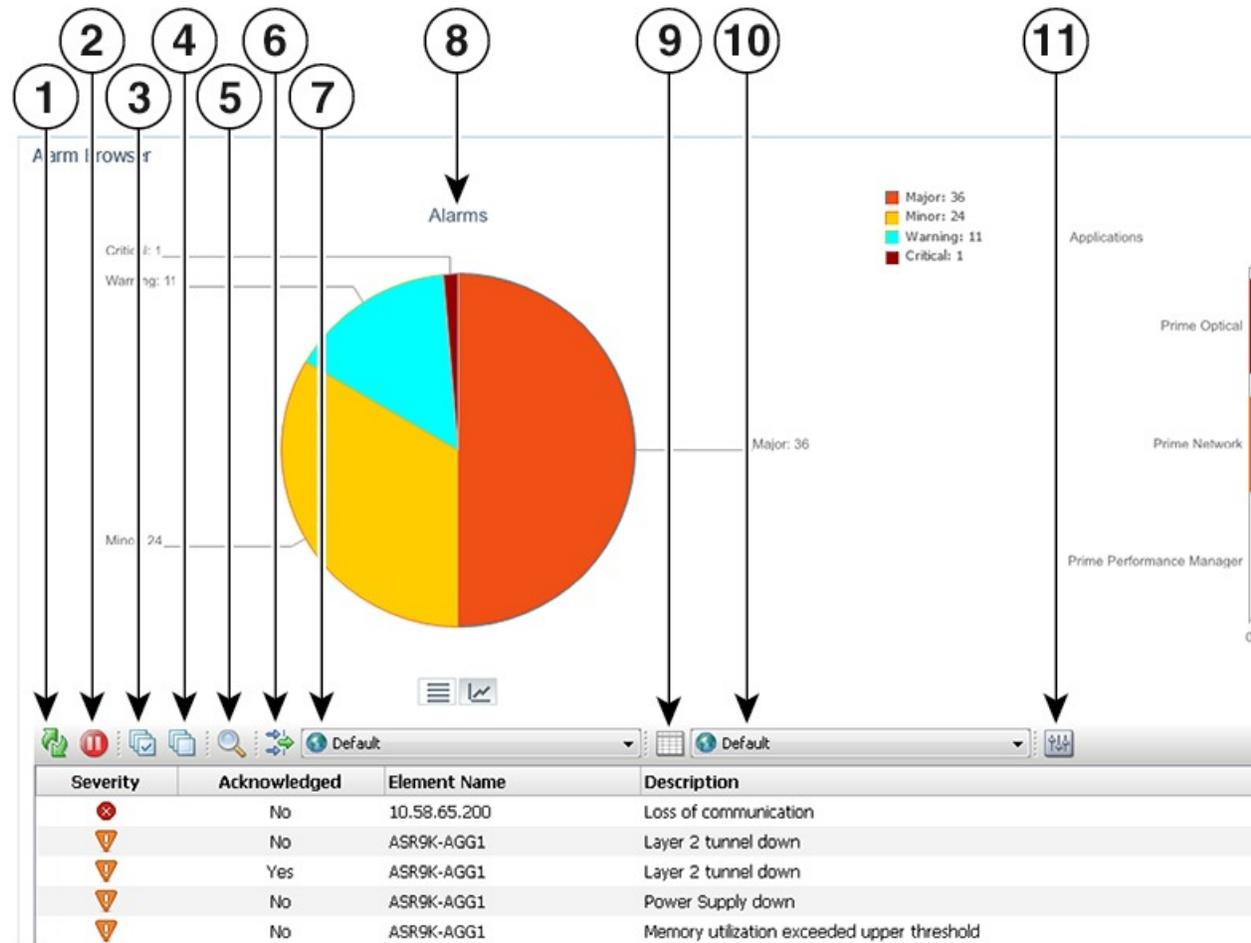
---

## Monitoring Affected Services and Customers

Prime Central provides an Alarm Browser portlet (see the following figure). Users with the Fault Management role and privileges can use the Alarm Browser to monitor and manage data about faults in the network. Information about alarms is displayed in the portlet according to filters and views:

- Filters let you display a subset of alerts based on specific criteria.
- Views let you choose which alert fields to display.

Figure 38: Alarm Browser Portlet



|   |  |    |                              |
|---|--|----|------------------------------|
| 1 | Refresh event data icon                                    | 9  | Edit Views ... icon          |
| 2 | Freeze/Unfreeze ... icon                                   | 10 | View list                    |
| 3 | Select all events icon                                     | 11 | Change preferences icon      |
| 4 | Deselect all events icon                                   | 12 | Alarms per Application chart |
| 5 | Find ... icon  | 13 | Table View icon              |
| 6 | Edit Filters ... icon                                      | 14 | Chart View icon              |
| 7 | Filter list  | 15 | Properties pane              |
| 8 | Alarms chart, which lists the number of alarms by severity | —  | —                            |

## Opening the Alarm Browser Portlet

To open the Alarm Browser portlet to display aggregated, deduplicated, and correlated active alarms:

### Procedure

**Step 1** From the Prime Central menu, choose **Assure > Prime Central Fault Management > Alarm Browser**.

You must have the appropriate role and privileges to open the Alarm Browser. If not, the following message is displayed:

You do not have access privileges to use the Fault Management component. Contact your administrator for access.

**Step 2** The first time you open the Alarm Browser, you must accept the self-signed, untrusted security certificates.

#### Mozilla Firefox

To accept the security certificates in Firefox, do the following:

- a) At the “This Connection is Untrusted” security prompt, right-click the frame behind the popup message and choose **This Frame > Open Frame in New Tab**.

The security certificate opens in a new browser tab.

- b) Click **I Understand the Risks**.
- c) Click **Add Exception**.
- d) In the Add Security Exception dialog box, make sure the **Permanently store this exception** check box is checked. (If you leave it unchecked, you will have to reaccept the security certificates the next time you launch the Alarm Browser.) Then, click **Confirm Security Exception**.
- e) Close the new tab, return to the Prime Central portal tab, and click the **Refresh Current Page** icon.
- f) In the Warning - Security dialog box, check the **Always trust content from this publisher** check box. (If you leave it unchecked, you will have to reaccept the security certificates the next time you launch the Alarm Browser.) Then, click **Yes** to the following message:

The web site's certificate cannot be verified. Do you want to continue?

**Note** If you click **No**, the security certificate is denied, and the Alarm Browser displays the error `The application failed to run`.

#### Microsoft Internet Explorer 10 and 11

**Note** If you have already applied CA Signed Certificates in Internet Explorer 10 or 11, then do not follow the below mentioned steps.

To accept the security certificates in Internet Explorer, do the following:

- a) Open Prime Central Fault Management login window in a new tab by entering the following URL:  
`http://Fault-Management-server-IP-address:Fault-Management-web-service-listener-port/primefm/console`

**Note** The Prime Central Fault Management web service listener port is 16311.

- b) Click **Certificate Error** in the browser's address bar, the Untrusted Certificate dialog box opens.
- c) Click **View Certificates** and click on **Certification Path** tab.
- d) The Certificate dialog box opens. Select first certificate (root certificate) and click **View Certificate**.

- e) Click **Install Certificate** to launch the certificate import wizard.
- f) Click **Next**.
- g) Select the **Place all certificates in the following store** radio button option and then click **Browse**.
- h) Navigate to the **Trusted Root Certification Authorities** folder and select it.
- i) Click **OK**.
- j) Click **Next**.
- k) Click **Finish** to complete the wizard.  
A security warning appears.
- l) Click **Yes** to confirm that you want to install the certificate.  
A message appears, indicating that the certificate import was successful.
- m) Click **OK** to close the message.
- n) Click **OK** to close the Certificate dialog box.
- o) Close the new tab, return to the Prime Central portal tab, and click the **Refresh Current Page** icon.

**Note** To view Alarm Reports in Internet Explorer 10, perform the following steps:

1. In the Browser window, go to **Tools > F12 Developer Tools**.
2. Change the **Browser Mode** to Internet Explorer 9.
3. Change the **Document Mode** to Internet Explorer 9 standards.

**Step 3** (Optional) You can replace the Prime Central certificates with your company's signed, trusted certificates. See [Managing the Self-Signed Certificates](#).

---

## Information Displayed in the Alarm Browser Portlet

The Alarm Browser portlet displays the following charts:

- Alarms—Displays in pie chart format the total number of alarms of each severity (critical, major, minor, and warning) for all applications combined.
- Alarms per Application—Displays in bar chart format the number of critical, major, minor, and warning alarms for individual applications.
  - The vertical axis (y-axis) shows the application.
  - The horizontal axis (x-axis) shows the alarm count.



---

**Note** If Prime Performance Manager is registered with Prime Central and sends alarms to Prime Central Fault Management, the Alarms per Application chart includes Prime Performance Manager. If Prime Performance Manager is configured to send alarms directly to Prime Network, there is no bar chart for Prime Performance Manager.

---

The table on the bottom half of the portlet displays the following information by default.

Table 18: Field Descriptions for the Alarm Browser Portlet

| Field            | Description   |
|------------------|---|
| Severity         | Severity of the selected alarm:   |
|                  | Critical alarm (red)  |
|                  | Major alarm (orange)  |
|                  | Minor alarm (amber)   |
|                  | Warning alarm (turquoise)   |
|                  | Indeterminate alarm (blue)  |
|                  | Cleared, normal, or OK (green)  |
| Acknowledged     | <p>Whether the selected alarm has been acknowledged in Prime Central. Values are Yes or No.</p> <p><b>Note</b> Prime Network changes alarm acknowledge state to <b>Modified</b>, if a new event is correlated to an acknowledged ticket. Prime Central GUI shows <b>Yes</b> or <b>No</b> indicating <b>Acknowledged</b> or <b>Unacknowledged</b> respectively (Modified state in Prime Central is internally mapped to Unacknowledged).</p> |
| Element Name     | Name of the device where the selected alarm occurred.   |
| Description      | Error message or condition that is associated with the selected alarm.  |
| Location         | Physical location of the equipment where the selected alarm occurred, such as chassis, rack, subrack (shelf), slot, and port numbers.   |
| Last Occurrence  | Time stamp when the alarm last occurred.  |
| Customer         | Name of the customer affected by the alarm.   |
| Service          | Name of the service affected by the alarm.  |
| Source           | Name of the application where the selected alarm originated.  |
| Element IP       | IP address of the device where the selected alarm occurred.   |
| VM Name          | Name of the VM where the selected alarm occurred.   |
| Host Server Name | Name of the host server where the selected alarm occurred.  |
| Count            | Number of times the alarm occurred.   |
| Has Correlated   | Whether the selected alarm has correlated alarms associated with it.  |
| EventId          | Unique identifier assigned to the selected alarm by the application where the alarm originated.   |

| Field  | Description   |
|--------|---|
| Serial | Unique identifier assigned to the selected alarm by the Fault Management component. Use this value when sending requests via the NBI API. |

The Alarm Browser's right-click menu options provide centralized alarm lifecycle management for the applications listed in the following table.

| Right-Click Menu Option | Supported by... |                  |                           | For More Information, See...                              |
|-------------------------|-----------------|------------------|---------------------------|---|
|                         | Prime Network   | Prime Optical    | Prime Performance Manager |   |
| —                       |                 |                  |                           | —   |
| Acknowledge             | Yes             | Yes              | Yes                       | <a href="#">Acknowledging or Deacknowledging an Alarm</a> |
| Deacknowledge           | Yes             | Yes              | Yes                       | <a href="#">Acknowledging or Deacknowledging an Alarm</a> |
| Clear                   | Yes             | Yes <sup>1</sup> | Yes                       | <a href="#">Clearing an Alarm</a>                         |
| Retire                  | Yes             | No               | Yes                       | <a href="#">Retiring an Alarm</a>                         |
| Add to Journal          | Yes             | Yes              | Yes                       | <a href="#">Adding Notes to an Alarm</a>                  |
| Resync Domain Managers  | Yes             | Yes              | Yes                       | <a href="#">Resynchronizing Applications</a>              |

<sup>1</sup> Please refer to the [Prime Optical 10.0 User Guide](#) for a listing of the alarms that can be cleared.



#### Note

- If the Alarm Management action you performed is not reflected in the Alarm Browser after refreshing it, review the Message Center for any errors that may have occurred.
- For Prime Network Tickets, Informational Severity is represented as Indeterminate Severity.

## Cross-Application Alarm Management

When configured for Suite Mode, previous releases of Prime Central, Prime Network, Prime Optical, and Prime Performance Manager supported the following cross-application alarm management tasks from the Prime Central Fault Management GUI:

- Acknowledge
- Deacknowledge
- Add Notes
- Clear
- Retire

Starting with the latest release of these applications, you can also perform these tasks from Prime Network, Prime Optical, and Prime Performance Manager (again, when configured for Suite Mode).



---

**Note** The Retire option is not supported by Prime Optical.

---

In addition, you have the ability to attach a note to any of these tasks from both the Prime Central Fault Management GUI and NBI. Keep in mind that the applications handle notes differently. Prime Central, Prime Network, and Prime Optical store the notes and actions associated with an alarm as journal entries, logging the creation or modification date and the relevant user's ID for each entry, whereas Prime Performance Manager stores a single note that can be modified as often as needed. Here are some other key differences in the way that the applications handle notes:

- A journal entry with the appropriate action prefix is created for all alarm management tasks performed from the Prime Central Fault Management GUI or NBI. For example, acknowledging an alarm results in a journal entry prefixed with `Acknowledge_Alarm:`.
- A journal entry is not created for any tasks (except for Add Notes) performed from Prime Network, Prime Optical, or Prime Performance Manager.
- When you add a note to an alarm from Prime Network, Prime Optical, or Prime Performance Manager, the corresponding journal entry is not prepended with an action prefix.
- In the alarm notifications sent by Prime Optical, there is no way to distinguish between notes generated in Prime Optical and notes generated in Prime Central. As a result, the journal entries for notes created in Prime Central for Prime Optical alarms are not prepended with an action prefix.
- Unlike Prime Network and Prime Optical, Prime Performance Manager keeps only one note per alarm. Prime Central journals each alarm management action (such as acknowledging or clearing an alarm) that is performed on a Prime Performance Manager alarm, but maintains only one journal entry for each Prime Performance Manager alarm note. For example, when a note is generated by Prime Performance Manager, Prime Central creates a journal entry for that same note. If the note is later modified within Prime Performance Manager, Prime Central overwrites the previous journal entry with the new entry.



---

**Note** Prime Performance Manager sends alarm note updates to Prime Central even if the updates are generated for alarm management actions carried out in Prime Central. As a result, it may appear that duplicate notes are listed in the Alarm Browser journal—this is normal. Prime Central maintains a journal entry for each alarm management action note it generates and a separate single journal entry for alarm notes generated by Prime Performance Manager.

---

For more information on notes, see [Adding Notes to an Alarm](#).

## Accessing Additional Alarm Information

From the Alarm Browser portlet, you can access more detailed information for a specific alarm by doing the following:

## Procedure

---

- Step 1** Right-click an alarm and choose **Device Details**. Depending on the alarm source, Prime Optical, Prime Network, or Prime Performance Manager launches, allowing you to view detailed alarm information at the application level.
- For information about using Prime Network to manage alarms and events, see the [Prime Network 4.3.2 Administrator Guide](#).
  - For information about using Prime Optical to view alarm information, see the “Managing Faults” chapter in the [Cisco Prime Optical 10.6 User Guide](#).
  - For information about using Prime Performance Manager to view alarm information, see the “Managing Network Alarms and Events” chapter in the [Cisco Prime Performance Manager 1.7 User Guide](#).
- Step 2** Right-click an alarm and choose **Ticket Details**. Prime Network launches and displays additional information for the ticket associated with the selected alarm. See the "Viewing Ticket Properties" topic in the [Cisco Prime Network 4.3.2 User Guide](#) for a description of the information provided.
- Note** This option is available only when you select an alarm that originated in Prime Network.
- Step 3** Right-click an alarm in the table and choose **Common Inventory**. The Common Inventory portlet launches, where you can view detailed information about the device on which the selected alarm occurred. For more information, see [What Is Inventory Management?](#)
- Step 4** Right-click an alarm in the table and choose **Correlated Alarms** to view alarms that are correlated to the selected alarm.
- Prime Central identifies the relationship between a root cause alarm and its consequent alarms. It automatically correlates the consequent alarms as children of the root alarm. The Alarm Browser displays the root cause alarm, the aggregated severity of the alarm, and the severity of the root cause alarm. In addition, the Alarm Browser displays the time at which the original alarm was detected.
- Step 5** Right-click a service-impacting alarm in the table and choose **Symptom Events** to see which symptom events are affected by the service-impacting alarm. The filtered view shows the causal relationship between an event and the consequent events that occurred because of it.
- Step 6** Right-click an alarm and choose **Subtending Events**. The Subtending Events window launches, listing all of the network events associated with the selected alarm and providing information for those events.
- Note** This option is available only when you select an alarm that originated in Prime Network.
- Step 7** Either double-click an alarm or right-click an alarm and choose **Information**. The Alarm Status for Serial Number *x* dialog opens, showing additional fields that are parsed from the alarm.
- Step 8** Right-click an alarm and choose **Journal**. The Journal Information for Serial Number *x* dialog opens, listing all of the notes that have been created for the selected alarm. For more information about notes, see [Cross-Application Alarm Management](#).
- 

## Viewing Alarms in the Alarm Summary

At the bottom of the Prime Central home page, users with the Fault Management role and privileges can view a summary of the alarm status of the network. Intended as a quick reference, the Alarm Summary shows the

total number of critical, major, minor, and warning alarms in the network—as do the charts in the Alarm Browser portlet.

You can change the rate at which the Alarm Summary refreshes automatically. Do the following:

### Procedure

---

**Step 1** Click within the Alarm Summary area.

**Step 2** In the Alarm Summary Timer dialog box, enter a refresh rate from 10 to 99,999 seconds. The default is 60 seconds.

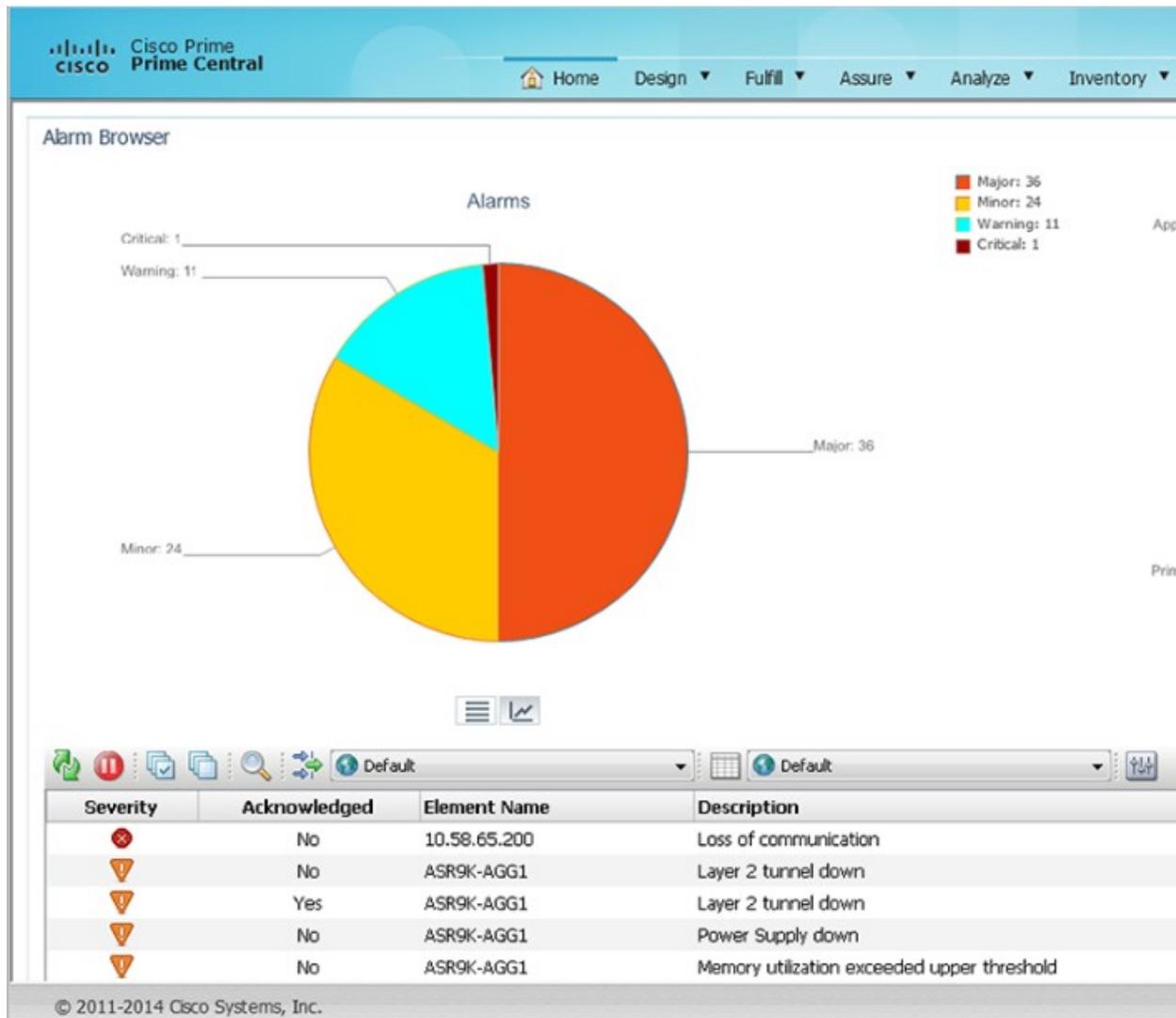
**Note** If you enter a value (such as 10abc) that cannot be parsed as a number, the refresh rate is reset to the last valid value. If you enter a number less than 10, the refresh rate is set to the lowest minimum, 10 seconds. You cannot enter a value higher than 99,999.

**Step 3** Click **Update**. The Alarm Summary refreshes at the rate you entered.

**Step 4** To stop the Alarm Summary from refreshing, reopen the Alarm Summary Timer dialog box and click **Stop**. (If later you decide to restart the automatic refresh, click **Start**.)

If you refresh your web browser, or if you log out of Prime Central and log back in, the Alarm Summary refresh rate resumes at the default 60 seconds, even if previously you had changed the refresh rate or stopped it altogether.

Figure 39: Alarm Summary



## Acknowledging or Deacknowledging an Alarm

Acknowledging an alarm indicates that you are aware of the issue and are taking ownership of it. The acknowledged alarm remains visible in Prime Central.

To acknowledge or deacknowledge alarms within Prime Central and propagate the change back to the application:

### Procedure

- Step 1** To acknowledge an alarm, right-click an alarm in the Alarm Browser and choose **Acknowledge**.

- Step 2** To deacknowledge a previously acknowledged alarm, right-click the alarm and choose **De-acknowledge**.
- Step 3** Refresh the Alarm Browser. The alarm is acknowledged (or deacknowledged) in Prime Central Fault Management, and the change propagates back to the application.
- 

## Clearing an Alarm

Cleared alarms remain in the Prime Central database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists. A cleared alarm means the alarm should no longer be considered a problem.

To manually clear an active alarm in Prime Central and propagate the change back to the application:

### Procedure

---

- Step 1** Right-click one or more alarms in the Alarm Browser and choose **Clear**.
- Step 2** Refresh the Alarm Browser. The alarm is cleared in Prime Central Fault Management, and the cleared condition propagates back to the application.

When you try to clear certain Prime Optical alarms, the Prime Central Message Center might show the following error message for the clear operation:

```
API_ERROR:clearAlarm operation failed. Reason: Unable to perform action on alarm IDs -
alarm IDs not found.
```

If the alarms exist in Prime Optical, you must clear them manually in Prime Optical. For a list of alarm categories that you must clear manually, see "EMS-Generated Alarms" in the [Cisco Prime Optical 10.6 User Guide](#), Chapter 9, "Managing Faults."

---

## Retiring an Alarm

To retire a cleared alarm in Prime Central and delete that same alarm from the application:

### Procedure

---

- Step 1** Right-click one or more alarms in the Alarm Browser and choose **Retire**. (Alarms must be cleared before they can be retired.)
- Step 2** At the confirmation prompt, click **OK**.
- Step 3** Refresh the Alarm Browser. The retired alarm is deleted from Prime Central and from the application.

**Note** Deleting an alarm from the Fault Management Alarm Browser will not delete the alarm from corresponding domain managers. It deletes it from only Prime Central and if a resync operation is done, the alarm re-appears in the Fault Management alarm browser.

---

## Adding Notes to an Alarm

You can add and save your own alarm history information. You can maintain a journal for any alarm.

To add notes to an alarm and propagate the note back to the application:

### Procedure

---

- Step 1** Right-click one or more alarms in the Alarm Browser and choose **Add to Journal**. The Journal dialog box opens.
- Step 2** Enter a note of up to 4000 characters.
- Step 3** Click **Save** to save the newly entered text and close the dialog box. The alarm note is saved in Prime Central and propagates back to the application.
- Step 4** To view an alarm note in Prime Central:
- Right-click one or more alarms and choose **Journal**. The journal shows the alarm note, the name of the user who entered it, and the date and time of the entry.
  - If you selected multiple alarms in the alarm list, click **Previous** or **Next** to move to the alarm note for the previous or next alarm in your selection.
  - Click **Close**.

**Note** For information on how Prime Central and other Prime applications handle notes, see [Cross-Application Alarm Management](#).

---

## Resynchronizing Applications

Complete the following procedure to resynchronize the alarm information provided by Prime Central and the Prime applications associated with it. Before you do so, be aware that:

- This feature is available only for applications that support resynchronization with the Prime Central Fault Management component.
- To initiate resynchronization from the right-click menu, at least one alarm must be reported in the Alarm Browser. If no alarms are present, initiate resynchronization by entering the following commands on the Fault Management server:

```
su - primeusr
```

```
fmctl resync
```

- Resynchronization status is not indicated in either the Message Center or Audit Log.

### Procedure

---

- Step 1** In the Alarm Browser, select an alarm and right-click it to open the right-click menu.
- Step 2** Select **Resync Domain Managers**.
- Step 3** To confirm that resynchronization started and completed, enter the following command on the Fault Management server to view the log file:

```
# tail -f ~/faultmgmt/log/resync.log
```

---

## Sorting Columns

Note the following when you sort columns in the Alarm Browser:

- To sort a column in the Alarm Browser, click the column header once. The rows are sorted in ascending order.
- To sort in descending order, click the column header again.
- To unsort the column, click the column header a third time.
- To sort multiple columns, press **Ctrl** and click the required column headers. The sorting importance of the columns is indicated in square brackets ([ ]) in the column header. To alternate the sorting of individual columns within the selection between ascending and descending order, keep **Ctrl** pressed and click the column headers. To unsort the columns, release **Ctrl** and click any header from among the sorted columns. The previously sorted columns are unsorted; the column that you clicked is sorted in ascending order.
- To lock a column, right-click the column header and click **Lock Column**. The column is moved to the left side of the portlet, and remains visible when you scroll horizontally. To unlock the column, right-click the column header and click **Lock Column** again.

## Refreshing Data

The alarm list refreshes automatically at regular intervals to show all incoming alerts from the Prime Central integration layer. You can choose to refresh the alarm list manually between the configured intervals to view all the latest alerts at the current point in time.

To refresh the Alarm Browser manually between automatic refresh updates, click the **Refresh** icon in the toolbar.

## Finding Data

Use the Find dialog box to search for specific text within the data in the Alarm Browser by doing the following:

### Procedure

---

- Step 1** In the Alarm Browser toolbar, click the **Find** icon.
- Step 2** In the Find dialog box, do the following:
- a) In the Column list, select the column to search.
  - b) In the Value field, enter the search value that you want to match. You can enter an exact value to search for or a regular expression.
  - c) In the Options area, specify the type of match required:
    - **Exact Match**—To find rows where the data in the selected column exactly matches the specified search value.
    - **Regular Expression**—To find rows where the data in the selected column matches the specified regular expression.

- Sub String—To find rows where the data in the selected column contains the specified value somewhere within it.
- d) Click **Find** to find the first matching occurrence.
- If a matching row is found in the Alarm Browser, any currently selected rows are deselected, and the matching row is selected. The Find dialog box remains open so that you can view any additional matching occurrences.
- e) Click **Next** to show the next match, and subsequent matches, in the Alarm Browser.
- f) Click **Close** to close the Find dialog box.
- 

## Changing the Alarm Information Displayed

You can set what alarm information is displayed from the available data by editing the list view, or by selecting and applying a different view. You can also edit the filter criteria used by the current alarm list, or select a different filter to apply to the alarm list.

From the Alarm Browser, do any of the following:

- To select a different view to apply to the alarm list, click the View drop-down list on the toolbar and select from the list of available views.
- To edit the current view and change the columns displayed, click **Edit Views**. The View Builder opens, which you can use to edit the view. See [Creating and Editing Views](#).
- To select a different filter to apply to the alarm list, select an available filter from the Filter list.  
For example, from the Filter list, choose **Service Impact Alarms** to view which customers and services are impacted by a specific alarm.
- To edit the current filter, click **Edit Filters**. The Filter Builder opens. See [Filtering Alarms Using the Advanced Filter](#).

## Filtering Alarms Using the Quick Filter

You can use the quick filtering facility as a fast way of displaying alarms that match a selected criteria. You can filter for alarm data and display alarms that correspond to the value of a specific cell. For example, you can quickly display only those alarms that occurred at the same time as the selected alarm, or before the selected alarm.

To filter alarms using the quick filter:

### Procedure

- 
- Step 1** In the Alarm Browser portlet, right-click a cell that contains a value on which to base the quick filter.
- Step 2** From the right-click menu, choose **Quick Filter** and select a submenu option.
- Step 3** To remove quick filtering and restore the portlet to its original view of all alarms, right-click a cell again and choose **Quick Filter > Off**.
-

## Filtering Alarms Using the Advanced Filter

Network alarms typically create many alerts that are not of immediate importance to the personnel monitoring the system. Use advanced filters to control the alarm information that is displayed.

In the Alarm Browser, use the Filter drop-down list to filter alarm data by specific fields, such as Cleared Alarms.

To create and edit advanced filters for alarm data:




---

**Note** At the time of Disaster Recovery (DR) configuration, you should create the views manually in the Standby machine.

---

### Procedure

---

**Step 1** In the Alarm Browser toolbar, click the **Edit Filters** icon. The Filter Builder opens.

**Step 2** Do one of the following:

- To create a filter, click **New Filter**.
- To edit an existing filter, select the list that contains the required filter. After the list has refreshed, click the filter.

If you are editing an existing filter, skip Step 3.

**Caution** Do not delete the “Default” filter. Deleting the Default filter generates an error.

**Step 3** Select the users to whom you want to grant access to the filter, and click **OK**.

**Step 4** Specify the general properties for the filter:

- Name—Enter a name for the filter. The name cannot contain the following characters:

\$ ! % ^ & \* ( ) + = - ` ~ # @ ' : ; < > { } [ ] ? / \ | , " ' `

Note that you cannot change the name of a filter after you have created that filter.

- Default View—Select the view with which you want to associate the filter, or select the view that is associated with the filter. The default view is applied when you launch an Alarm Browser with the filter but do not specify a view.
- Collection—(For global filters and system filters only) Select the filter collection or collections to which you want to add the filter.
- Description—Enter a description that explains the purpose of the filter.
- Data Source—Select the data source or data sources that contain the fields against which you want to run queries. Click the **Show Data Sources** icon to display a list of available data sources.

If you are editing an existing filter, proceed to Step 8.

**Step 5** In the first row of the **Basic** tab, create a filter condition as follows:

- a) From the Field list, select a field from the specified data source.

- b) From the Comparator list, select a comparator.
- c) In the Value field, enter a numeric data type value, or a string data type value. The data types must correspond to those in the ObjectServer field. String data type entries in the Value field must be contained in single quotes.
- d) (Optional) Use the “like” and “not like” comparators for regular expression pattern-matching metacharacters against the entry in the Value field.

**Note** Do not use the getdate expression in the Value field.

**Step 6** To add additional filter conditions, click +. You can add as many filter conditions as required.

**Step 7** Use the match options to specify how the filter conditions combine in aggregate:

- Click **All** to trigger the filter only if all the conditions are met.
- Click **Any** to trigger the filter if any of the conditions are met.

**Step 8** (Optional) To preview the literal SQL WHERE clause output, click **Advanced**.

**Step 9** Click **Metric** and use the following fields to set the metric value:

- Label—Enter a title for the metric.
- Function—Select a function to perform on the field data.
- Field—Select a field on which to perform the chosen function.

**Step 10** Click **Save and Close**.

## Filter Builder Modes

You can use the following modes to create filters; the Filter Builder displays a tab for each mode after you click **New Filter**.

### Basic Mode

Basic mode provides a set of lists and text fields that you use to specify the filter conditions. To build the conditions, select a field from the specified data sources, select a comparator, and enter a numeric data type or string data type value. The data type value is used as the filtering criterion used against the field. If you use basic mode to construct your filter, you can view the resulting SQL in the text field on the Advanced tab.

The fields in the Basic tab map to the following columns in the Alarm Browser default view:

| This field name: | ... Maps to this Alarm Browser column title: |
|------------------|--|
| Severity         | Severity                                     |
| Acknowledged     | Acknowledged                                 |
| Node             | Element IP                                   |
| NodeAlias        | Element Name                                 |
| Summary          | Description                                  |
| AlertKey         | Location                                     |

| This field name: | ... Maps to this Alarm Browser column title: |
|------------------|--|
| LastOccurrence   | Last Occurrence                              |
| Tally            | Count  |
| Agent            | Source                                       |
| Customer         | Customer                                     |
| HasCorrelated    | Has Correlated                               |

### Advanced Mode

Provides a text field into which you can enter an SQL syntax. If you create a filter in advanced mode, it might not be possible to express the SQL syntax in the fields on the Basic tab. After you have saved a filter created in advanced mode, the Basic tab is removed for that filter.

### Dependent Mode

This tab is displayed only for dependent filters. On this tab, use the Search fields to identify the filters that you want to use for the dependencies. After you have identified the required filters, move the filters from the Available filters list to the Selected dependencies list. In a dependent filter, the SQL WHERE statements of each filter are concatenated by using OR statements.

### Metric Mode

A metric is an aggregate statistic that can be derived from the alerts that match a filter to display a useful figure; for example, an average, count, or sum of all field values. If a filter is displayed using a monitor box linked to an Alarm Browser, the metric information obtained from the set of alerts that match this filter is used for this display.

## Creating and Editing Views

Use the View Builder to create and edit views that are dynamically applied to Alarm Browser data. The views determine what information is displayed from the available alarm data.



**Note** At the time of Disaster Recovery (DR) configuration, you should create the views manually in the Standby machine.

### Procedure

**Step 1** In the Alarm Browser toolbar, click the **Edit Views** icon.

**Step 2** In the View Builder, do one of the following:

- To create a new view, click **New View**.
- To edit an existing view, select the desired view from the View list. The page updates with the view properties.

If you are editing an existing view, skip Step 3.

**Step 3** Select the users to whom you want to grant access to the view, and click **OK**.

**Step 4** Use the following fields to set the general properties for the view:

- **Name**—Enter a name for the view. The name cannot contain the following characters:

\$ ! % ^ & \* ( ) + = - ` ~ # @ ' : ; < > { } [ ] ? / \ | , "

By default, the following characters cannot be used as the initial character of a view name:

/ \ \* ? " < > | & .

- **Data Source**—Select the data source or data sources that contain the fields that you want to be displayed in the view. Click the **Show Data Sources** icon to display a list of available data sources.

**Step 5** Select the columns you want the Alarm Browser to display, and specify how those columns are ordered.

- In the Display Columns area, use the > and < arrows to move fields between lists. Only those fields in the Event list view list are visible as columns in the Alarm Browser.
- In the Event list view list, select a field.
- Use the arrow buttons to the right of the list to change the display order of the columns in the view:
  - Click **Top** to move the field to the top of the list. In the Alarm Browser, the field is displayed as the column furthest to the left.
  - Click **Up** to move the selected field up one position in the list.
  - Click **Down** to move the selected field down one position in the list.
  - Click **Bottom** to move the selected field to the bottom of the list. In the Alarm Browser, the field is displayed as the column furthest to the right.
- (Optional) Check the **Lock column** check box to lock the selected column at the far left of the Alarm Browser in the view, so that the column is always displayed when you scroll horizontally.
- (Optional) Select a field from the Event list view list and update the corresponding column's title, width, and alignment.

**Step 6** Click **Save and Close**.

## Freezing and Unfreezing the Alarm Browser

To take a snapshot of alarm information before it is changed by updates from the Prime Central integration layer, you can freeze all the fields on the Alarm Browser by doing the following:

### Procedure

**Step 1** To freeze the fields, click the **Freeze/Unfreeze** icon in the Alarm Browser toolbar.

The updates from the Prime Central integration layer are suppressed.

**Step 2** To unfreeze the fields and obtain updates from the Prime Central integration layer, click the **Freeze/Unfreeze** icon again.

**Step 3** (Optional) To force a refresh of the fields independently of the refresh rate, click the **Refresh** icon.

---

## Configuring Email and SMS for Alarm Notifications

You can configure Prime Central Fault Management to notify you whenever a critical or major alarm is generated. You can choose to receive either an email notification or a SMS notification sent to your cell phone.



**Note** Prime Central Fault Management uses the Linux sendmail function under /usr/sbin, /sbin, /usr/lib, /bin, or /usr/bin to send email notification.

---

### Procedure

---

**Step 1** As the primeusr user, log in to the Prime Central portal with the primeusr password that you specified during installation.

**Step 2** Change directories to the *installation-directory/faultmgmt* folder.

**Step 3** Open the .primefmmaillist file and add both the email addresses and phone numbers that you want to receive alarm notifications.

You can enter multiple email addresses and phone numbers on a single line, separated by a space. Entries for SMS message recipients should be formatted as follows:

*recipient's-mobile-number@carrier's-SMS-gateway-address*

**Note** To determine a carrier's SMS gateway address, either view this [page](#) or contact the carrier directly.

**Step 4** Save and close the .primefmmaillist file.

When a critical or major alarm occurs, you will receive an email or SMS message similar to the following:

```
From: PRIMEFM User [mailto:primeusr@cisco.com]
Sent: Monday, February 17, 2014 7:21 AM
To: John Doe
Subject: Prime Central Fault Management Email
This message refers to node <node-ID>, which has the following problem:
Loss of communication
```

```
The severity is Critical
Sent by Cisco Prime Central Fault Management
```

**Note** Ensure the sendmail and m4 packages are installed. You can install the sendmail and m4 packages using the following commands as root user:

```
# yum install sendmail sendmail-cf
# yum install m4
```

---

## Changing Alarm Browser Preferences

### Procedure

- 
- Step 1** In the Alarm Browser toolbar, click the **Change preferences** icon.
- Step 2** In the Preferences dialog box, click the **Monitor Boxes** tab and specify what information is displayed by the monitor boxes on the Alarm Browser.
- See [Preferences Dialog Box, on page 121](#) for a description of the options you can set in the Preferences dialog box.
- Step 3** Click the **Notifications** tab and configure preferences for alert notifications when the alarm list is minimized.
- Step 4** Click the **Flashing** tab and specify alarm list preferences for flashing on receipt of new alerts.
- Step 5** Click the **Event List** tab and set other alarm list preferences.
- Step 6** Click **Apply**.
- Step 7** Click **Save**; then, click **Close**.
- 

### Preferences Dialog Box

The following table describes the options you can set in the Alarm Browser's Preferences dialog box.

*Table 19: Preferences Dialog Box*

| Option                       | Description  |
|------------------------------|--|
| <b>Monitor Boxes Tab</b>     |  |
| Show Number of Alerts        | Displays the number of alerts that match the filter.   |
| Show Highest Severity        | Displays the highest severity of the alerts that match the filter.   |
| Show Lowest Severity         | Displays the lowest severity of the alerts that match the filter.  |
| Show Highest Severity Border | Displays a border around the monitor box in the color of the highest-severity alert that matches the filter.   |
| Show Metric                  | Displays the selected filter metric value.   |
| Show Highest Color           | (Applicable only if you selected the Show Highest Severity option) Displays the highest-severity alert indicator in the color of the alert: for example, in red if the highest-severity alert is critical. |
| Show Lowest Color            | (Applicable only if you selected the Show Lowest Severity option) Displays the lowest-severity alert indicator in the color of the alert.  |
| Font                         | Choose the font and the font size for the text on the monitor boxes.   |

| Option                    | Description   |
|---------------------------|---|
| Distribution meter        | Specify the format for the distribution meter: <ul style="list-style-type: none"> <li>• Show Lava Lamp—Displays the distribution meter as a series of horizontal bars.</li> <li>• Show Histogram—Displays the distribution meter as a bar graph.</li> <li>• Show None—Switches off the distribution meter.</li> </ul>   |
| <b>Notifications Tab</b>  |   |
| Enabled                   | Check this check box to receive notification of new, changed, or deleted alerts when the alarm list is minimized.   |
| When Iconized             | Click this radio button to receive notification of new, changed, or deleted alerts on iconized desktop environments. An iconized desktop environment displays an icon when the alarm list is minimized.   |
| Always                    | Click this radio button to always receive notification of new, changed, or deleted alerts.  |
| When                      | Check each check box to receive notification as follows: <ul style="list-style-type: none"> <li>• New—You receive a notification when a new alert is added to the alarm list.</li> <li>• Change—You receive a notification when an existing alert changes in the alarm list.</li> <li>• Delete—You receive a notification when an existing alert is deleted from the alarm list.</li> </ul> |
| How                       | Select each option to indicate how a notification should occur: <ul style="list-style-type: none"> <li>• Alert Icon—Flashes the minimized alarm list.</li> <li>• Open Window—Opens the alarm list on the window.</li> <li>• Play Sound—Plays a sound on the workstation.</li> <li>• Open URL—Opens a URL. In the URL Target field, enter the URL that you want to be opened.</li> </ul>     |
| <b>Flashing Tab</b>       |   |
| Enable Flashing check box | Check to enable alarm list flashing.  |
| Speed slider              | Use to indicate how quickly the alarm list flashes.   |
| Brightness slider         | Use to indicate the degree of brightness of the flashing.   |
| <b>Event List Tab</b>     |   |
| Show Colors               | Displays each row of the alarm list with a background color that corresponds to the severity of the alarm.  |

| Option                        | Description  |
|-------------------------------|--|
| Show Distribution Summary Bar | Displays the distribution summary bar, which shows the number of alerts that match each severity color.  |
| Show Toolbar                  | Makes the toolbar available on the alarm list.   |
| Font Name                     | Choose a font for your alarm list.   |
| Font Size                     | Choose a font size for your alarm list.  |
| Date Format                   | Choose the required date format. If you select Customize, enter a custom format.   |
| Time Zone                     | Choose a time zone from the available options.   |
| Event List Icons              | Specify how you want the alarm severity to be depicted in the Severity column: <ul style="list-style-type: none"> <li>• Show—Displays an icon to denote alarm severity.</li> <li>• Show With Text—Displays an icon and text to denote alarm severity.</li> <li>• Don't Show—Displays text to denote alarm severity.</li> </ul> |

### Customizing the Sound of Alarm Notifications

To set up the Play Sound option for audible notification:

#### Procedure

- 
- Step 1** Prepare the sound file and place it in the following directory on your server:  
*Fault-Management-installation-directory/faultmgmt/tipv2/profiles/TIPProfile/installedApps/TIPCell/isc.ear/OMNIBusWebGUI.war/sounds.*
- Step 2** In the Alarm Browser toolbar, click the **Change preferences** icon.
- Step 3** In the Notification area, check the **Enabled** check box.
- Step 4** In the Preferences dialog box, click the **Notifications** tab.
- Step 5** In the How area, check the **Play Sound** check box.
- Tip** To preview the default sound, click the **Play** button.
- Step 6** To change the default sound to the one you uploaded in Step 1, specify the sound file in the Play Sound field. Use the following format:  
**\$(SERVER)/sounds/<sound-filename>**  
For example:  
\$(SERVER)/sounds/crash.wav
- Step 7** Click **Apply**.

**Step 8** Click **Save**; then, click **Close**. The change takes effect when a new notification appears.

---

## Managing Prime Central Fault Sources

From the Fault Source Management portlet, you can identify and keep tabs on the sources from which Prime Central gathers your network's alarm and trap information. To view this portlet:

1. Ensure that you have have fault management privileges.
2. Add it to the Prime Central home page. See [Adding a Portlet](#) for instructions.

Note the following:

- After a source has been registered with Prime Central's fault management component, fault data for that source is displayed in the Alarm Browser portlet.
- All instances of Prime Network, Prime Optical, and Prime Performance Manager associated with Prime Central are automatically added to the Fault Source Management portlet. Also, these are the only fault sources that cannot be modified or removed from the portlet.

## Adding a Fault Source

### Procedure

---

**Step 1** From the Fault Source Management portlet, click **Add**.

The Add New Fault Source dialog box appears.

**Step 2** Enter the appropriate information and then click **OK**.

Note the following:

- A red asterisk denotes the fields that require user input.
- If you select the Resync Support check box, you will need to enter additional information.

See the [Add New Fault Source Dialog Box](#) for a description of the fields provided here.

---

## Editing a Fault Source

### Procedure

---

**Step 1** From the Fault Source Management portlet, select the fault source you want to modify and then click **Edit**.

The Edit Fault Source dialog box appears.

**Step 2** Make the necessary changes and then click **OK**.

**Note** You can edit everything except the source type.

See the [Add New Fault Source Dialog Box](#) for a description of the fields provided here.

## Deleting a Fault Source

### Procedure

- Step 1** From the Fault Source Management portlet, select the fault source you want to remove.
- Step 2** Click **Delete**.

## Add New Fault Source Dialog Box

The following table describes the fields that are provided in this dialog box.

| Field                  | Description   |
|------------------------|---|
| Type                   | Indicates the fault source type.  |
| Display Name           | Display name of the fault source, which is listed in the Fault Source Management portlet's Source column.   |
| Host Name              | Hostname of the fault source.   |
| Instance Name          | Instance name of the fault source.  |
| (Optional) Description | Description of the fault source.  |
| Version                | Version number of the fault source.   |
| (Optional) Patch       | Patch number of the fault source.   |
| Resync Support         | Indicates whether resync is enabled on the fault source.<br>When this option is selected, the data for a particular fault source is automatically synchronized whenever you restart Fault Management. |
| Resync URL             | URL of the fault source on which resync is enabled.   |
| User Name              | Username required to log in to the fault source.  |
| Password               | Password required to log in to the fault source.  |

## Analyzing Fault Data

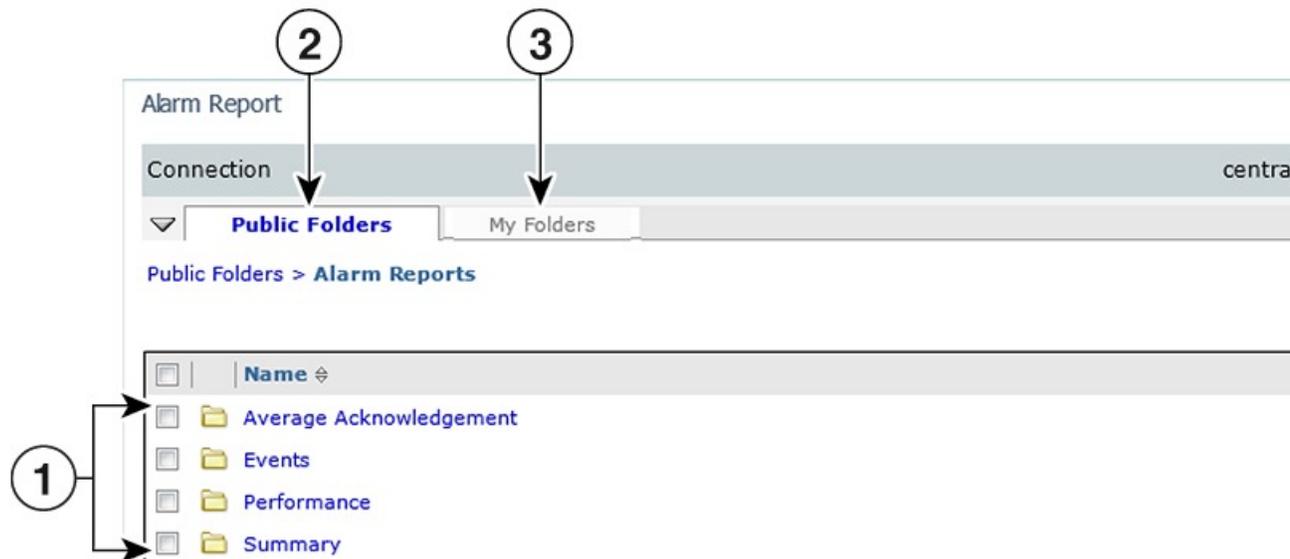
Prime Central provides an Alarm Report portlet (see the following figure) that lets you analyze fault data and help you make informed and timely decisions. Reports can be published to the portlet to ensure that everyone in your organization has accurate and relevant information when they need it.

The Alarm Report portlet shows an alarm summary and details grouped by node, severity, source application, and so on. Users with the appropriate role and privileges can view, customize, and schedule reports for active and historical alarms. You can export the generated reports in HTML, PDF, Excel, and PostScript format.

The Alarm Report portlet displays the following tabs:

- Public Folders—Reports that are placed in Public Folders are of interest to and can be viewed by many users.
- My Folders—You create personal folders and use them to organize reports according to your preferences. My Folders are accessible by you only when you are logged on.

Figure 40: Alarm Report Portlet



|   |                          |   |                     |
|---|--------------------------|---|---------------------|
| 1 | Predefined alarm reports | 6 | Set Properties icon |
| 2 | Public Folders tab       | 7 | Launch menu         |
| 3 | My Folders tab           | 8 | Order icon          |
| 4 | Refresh icon             | 9 | More link           |
| 5 | Delete icon              | — | —                   |



**Note** Report Studio is not supported in Prime Central 1.4. Also, the links under **Launch** menu are not supported.

## Default Alarm Reports

The Alarm Report portlet supports the predefined alarm reports shown in the following table.

Table 20: Default Alarm Reports

| Report Name                   | Description   | Purpose  |
|-------------------------------|---|--|
| <b>Average Acknowledgment</b> |   |  |
| Ack_Events_Details            | Shows a detailed breakdown of the average acknowledgment times within a network management environment for a specific user or group.                                      | Assists operators and managers in pinpointing and addressing discrepancies in acknowledgment rates across the network. |
| Ack_Events_Summary            | Shows the average acknowledgment times within a network management environment for all users and groups.  |  |
| <b>Events</b>                 |   |  |
| Events_Details                | Displays a detailed report of all events of a selected node, class, manager, alert group, or severity over a user-specified time period.                                  | Assists operators and managers in providing coverage for specific criteria in event management.                        |
| Events_Summary                | Displays the highest event-generating elements based on either node, class, manager, alert group, or severity over a user-specified time period.                          | Helps identify low performance of a system or server over a period of time.  |
| <b>Performance</b>            |   |  |
| Perf_Details                  | Generates a supplementary drill-down report of a selected operator, group, class, or manager over a user-specified time period.   | Helps identify the most overloaded owner, class, or event manager, and assists in identifying performance issues.      |
| Perf_Summary                  | Generates a bar chart and supplementary drill-down table displaying the number of events handled by either an owner, class, or manager over a user-specified time period. |  |
| <b>Summary</b>                |   |  |
| Get_All_Journals              | Retrieves all journal entries associated with a specific node.  | Allows users to track journal or state change information about specific nodes and devices that have generated events. |

## Opening the Alarm Report Portlet



**Tip** If multiple users plan to share the same browser instance and use the Alarm Report portlet, it is recommended that those users clear their browser cache before logging in to Prime Central.

To open the Alarm Report portlet:

## Procedure

---

**Step 1** From the Prime Central menu, choose **Assure > Prime Central Fault Management > Alarm Report**.

If you do not have the appropriate role and privileges to open the Alarm Report, the following message is displayed:

You do not have access privileges to use the Fault Management component. Contact your administrator for access.

**Step 2** The first time you open the Alarm Report, you must accept the self-signed, untrusted security certificates.

### Mozilla Firefox

To accept the security certificates in Firefox, do the following:

- a) At the “This Connection is Untrusted” security prompt, right-click the frame behind the popup message and choose **This Frame > Open Frame in New Tab**.  
The security certificate opens in a new browser tab.
- b) Click **I Understand the Risks**.
- c) Click **Add Exception**.
- d) In the Add Security Exception dialog box, make sure the **Permanently store this exception** check box is checked. (If you leave it unchecked, you will have to reaccept the security certificates the next time you launch the Alarm Report.) Then, click **Confirm Security Exception**.
- e) Close the new tab, return to the Prime Central portal tab, and click the **Refresh Current Page** icon.
- f) In the Warning - Security dialog box, check the **Always trust content from this publisher** check box. (If you leave it unchecked, you will have to reaccept the security certificates the next time you launch the Alarm Report.) Then, click **Yes** to the following message:

The web site's certificate cannot be verified. Do you want to continue?

**Note** If you click No, the security certificate is denied, and the Alarm Report displays the error “The application failed to run.”

### Microsoft Internet Explorer

To accept the security certificates in Internet Explorer, do the following:

- a) At the security prompt, click **Continue to this website**.
- b) In the Internet Explorer Information Bar, choose **Display Blocked Content**.
- c) In the Warning - Security dialog box, check the **Always trust content from this publisher** check box. (If you leave it unchecked, you will have to reaccept the security certificates the next time you launch the Alarm Report.) Then, click **Yes** to the following message:

The web site's certificate cannot be verified. Do you want to continue?

**Note** If you click No, the security certificate is denied, and the Alarm Report displays the error “The application failed to run.”

**Step 3** (Optional) You can replace the Prime Central certificates with your company's signed, trusted certificates. See [Managing the Self-Signed Certificates](#).

---

## Creating a New Report

### Procedure

---

- Step 1** In the Alarm Report portlet, click **Launch > Report Studio**.
- Report Studio is a web product for creating reports that analyze corporate data according to specific information needs.
- Step 2** Click **Create a new report or template**.
- Step 3** Choose the desired report template; then, click **OK**.
- Step 4** Select the data items you want to appear in your report:
- In the Insertable Objects pane, on the Toolbox tab, drag **Singleton** to the report.  
An empty data container is created.
  - From the Insertable Objects pane, on the Source tab, drag a data item into the singleton container. To create a singleton, you can also drag a data item anywhere in your report layout.
  - To change the query associated to the singleton object, in the Properties pane, double-click the **Query** property and make changes.
- Step 5** From the **Run** menu, click one of the options to produce the report in the format you want.
- You can produce a report in HTML, PDF, CSV, various Excel formats, and XML. You cannot produce a report in CSV format if you have more than one query defined in the report unless the additional queries are used for prompts.
- The report runs. Once the report has finished running, you can run the report again in the same format or in a different format. If you run the report again in CSV or XLS format, the report will appear in a new browser window.
- 

## Scheduling a Report

You can set up a schedule to run a report at a later time or at a recurring date and time.

If you no longer need a schedule, you can delete it. You can also disable it without losing any scheduling details. You can then enable the schedule at a later time.

### Procedure

---

- Step 1** Drill down to the report for which you want to set up a schedule; for example, **Public Folders > Alarm Reports > Events > Events\_Details**.
- Step 2** Click the **Schedule - report name** icon.
- Step 3** Specify the schedule parameters:
- Under Priority, lower numbers designate higher priority. The default priority setting is 3.
  - To create the schedule but not apply it right away, check the **Disable the schedule** check box. To enable it later, uncheck the check box.

**Step 4** Click **OK**.

A schedule is created and the report runs at the next scheduled time.

**Step 5** After clicking OK, you might receive the following “Renew the credentials” prompt:

```
The user or password you provided is not valid. Provide valid credentials.
```

If you enter the password you used to log in to Prime Central and click **OK**, the dialog box remains open, and the password field becomes blank. If you click **OK** without entering a password, or if you click **Cancel**, the dialog box closes, but the scheduled report fails to run because of a password authentication failure.

Do the following:

1. As the primeusr user, log in to the Prime Central Fault Management server.
2. Change directories to the faultmgmt/prime\_integrator/scripts/ directory.
3. Run the updatePasswdForReporting.sh script, which lets you provide the username and password to use for report scheduling.

For example, enter:

```
# updatePasswdForReporting.sh centraladmin Admin
```

where:

- centraladmin is the username to use when scheduling a report.
  - Admin is the password to use when scheduling a report.
4. Return to the “Renew the credentials” prompt and in the Password field, enter the password you configured in the previous step; then, click **OK**.

A schedule is created and the report runs at the next scheduled time.

**Step 6** The next time you schedule a report, you do not have to rerun the updatePasswdForReporting.sh script or renew your credentials. However, if *someone else* runs the script and changes the report scheduling password, you must renew your credentials again. To do this:

- a) In the Alarm Report portlet, click the **My Area** icon and then choose **My Preferences**.
- b) In the Set preferences dialog box, click the **Personal** tab.
- c) Scroll down to the Credentials area and click **Renew the credentials**.

A message appears, indicating that the credentials have been renewed with your username and password.

- d) Click **OK**.

---

## Saving or Emailing a Report

You can distribute reports to other users by:

- Saving them where other users can access the reports at their convenience, such as in the public folders. Public folders typically contain reports that are of interest to many users.
- Sending them to users by email. This is especially useful if you want to share the report with a group of people who do not have access to the Alarm Report portlet.

To save or email a report:

### Procedure

---

- Step 1** Open the report that you want to save or email; for example, **Public Folders > Alarm Reports > Average Acknowledgement > Ack\_Events\_Summary**.
- Step 2** To save the report:
- In the report toolbar, choose **Keep this version > Save as Report View**.
  - Enter a name for the report.
  - Accept the default location, or click **Select another location**.
  - Click **OK**.
- Step 3** To email the report:
- In the report toolbar, choose **Keep this version > Email Report**.
  - Enter the recipient's email address.
  - Check the following check boxes:
    - Include a link to the report**—To include a URL to the report in the email.
    - Attach the report**—To attach the report to the email.
  - Click **OK**.
- 

## Setting Report Properties

You can control the way a report appears and behaves by modifying its properties. To do so:

### Procedure

---

- Step 1** Drill down to the report for which you want to set properties; for example, **Public Folders > Alarm Reports > Events > Events\_Summary**.
- Step 2** In the report's Actions toolbar, click **Set properties - report name**.
- Step 3** Click the **General** tab and make any necessary changes to settings such as the report's owner, display icon, and name.
- Step 4** Click the **Report** tab and set the default action that is taken on the report.
- Step 5** Click the **Permissions** tab and specify which users and groups have access to the report, as well as the actions they can perform on the content.
- Step 6** Click **OK**.
- 

## Specifying the Report Order

You can specify the order of reports in the Alarm Report portlet. You might decide to organize reports by level of usage and place reports that you use daily at the top of the list.

By default, existing reports are sorted alphabetically. Reports added after the order is specified are shown at the end of the list.

### Procedure

---

- Step 1** In the Alarm Report toolbar, click **Order**.
  - Step 2** Select the reports in the “Shown in default order” list box and click the right-arrow button to move them to the “Shown first” list box.
  - Step 3** Click the **Up**, **Down**, **To top**, and **To bottom** links to move the reports within the list.
  - Step 4** Click **OK**.
- 

## Deleting a Report

### Procedure

---

- Step 1** Drill down to the report that you want to delete; for example, **Public Folders > Alarm Reports > Summary > Get\_All\_Journals**.
  - Step 2** Check the check box to the left of the report.
  - Step 3** In the toolbar, click **Delete**.
  - Step 4** At the confirmation prompt, click **OK**.
- 

## Configuring Alarms Retention Period

To retain the historical alarms data for more than 14 days (which is the default period), configure the retention period using **Options** section in **Alarms Report** portlet. After the configuration details are saved, the scheduler is triggered periodically to remove the historical data, which is older than the configured retention period.



### Note

- By default, the historical alarms report data is retained for 14 days.
  - Increasing alarm retention period will consume more database resources.
  - The historical data can be retained to any number of days. But, more than 90 days of retention period may lead to performance issues.
- 

### Procedure

---

- Step 1** In the **Alarms Report** portlet, at the top right corner, click **Options** and choose **Configuration**.
- Step 2** Click **Edit**.
- Step 3** Specify the retention period and click **Save**.

The allowed retention period range is 1-99999.

## Configuring the SNMP Gateway for NBI Integration

### Procedure

- Step 1** As the primeusr user, log in to the Prime Central Fault Management server.
- Step 2** Copy the example properties file, NCO\_GATE.props, from the \$OMNIHOME/gates/snmp directory to the \$OMNIHOME/etc directory.
- Step 3** In the NCO\_GATE.props file, change the values of the gateway-specific properties to suit your operating environment. The gateway-specific properties are listed in the following table:
- Note** A new name has been introduced for SNMP gateway process in which is to change the value of the property "Name" as 'G\_SNMP'.
- Step 4** Enter the following command to start the SNMP gateway:
- ```
nco_g_snmp &
```

### Gateway-Specific Properties

The following table lists the properties you can modify when configuring an SNMP gateway for NBI integration.

**Table 21: Gateway-Specific Properties**

| Property Name                             | Command-Line Option                   | Description                                                                                                                                                                                                                                                       |
|-------------------------------------------|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gate.SNMPCommunity<br><i>string</i>       | -snmpcommunity<br><i>string</i>       | Community string from SNMP traps. The default is public.                                                                                                                                                                                                          |
| Gate.SNMPEnableLookup<br><i>boolean</i>   | -snmpenablelookup<br><i>boolean</i>   | Whether or not host lookup is enabled. The default is TRUE.                                                                                                                                                                                                       |
| Gate.SNMP.EngineID<br><i>string</i>       | -snmpengineid<br><i>string</i>        | Gateway engine ID, which identifies the gateway as the source of the SNMPv3 traps. The default is 0x0102030405.<br><br><b>Note</b> This property is used only with SNMPv3 traps and must match the engine ID specified in the configuration file of the receiver. |
| Gate.SNMPForwardUpdates<br><i>boolean</i> | -snmpforwardupdates<br><i>boolean</i> | Whether or not the gateway forwards alert updates to the ObjectServer. In effect, the original alert is duplicated but will include the updated data. The default is FALSE.                                                                                       |

| Property Name                            | Command-Line Option                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gate.SNMP.Gateway<br><i>string</i>       | -snmpgateway <i>string</i>          | <p>IP address and port to which the gateway forwards traps. The default is 127.0.0.1:162.</p> <p>If you are operating in an IPv4 environment, specify the location in IPv4 format as <i>address:port</i>. For example:<br/>127.0.0.1:8080</p> <p>If you are operating in an IPv6 environment, specify the location in IPv6 format, preceded by tcp6 or udp6, and followed by the port number, as tcp6 udp6:<i>address:port</i>. For example:<br/>tcp6:[::01]:6666</p> |
| Gate.SNMP.OID<br><i>string</i>           | -snmpoid <i>string</i>              | <p>Object identifier (OID) for traps. The default is 1.3.6.1.4.1.1279 (an IANA-registered Private Enterprise Number).</p> <p>This property can also be defined as @NodeGroup to forward the value of the NodeGroup column in the status table.</p>                                                                                                                                                                                                                    |
| Gate.SNMP.Protocol<br><i>string</i>      | -snmpprotocol <i>string</i>         | <p>Transport protocol that the gateway uses:</p> <ul style="list-style-type: none"> <li>• TCP—Transmission Control Protocol.</li> <li>• UDP—(Default) User Datagram Protocol.</li> </ul> <p><b>Note</b> Store-and-forward mode is not available when the gateway uses UDP.</p>                                                                                                                                                                                        |
| Gate.SNMP.Retries<br><i>integer</i>      | -snmpretries <i>integer</i>         | <p>Number of times that the gateway attempts to retry sending a message on failure. When this number is exceeded, the gateway stops sending messages to the port. The default is 5.</p>                                                                                                                                                                                                                                                                               |
| Gate.SNMP.SecurityLevel<br><i>string</i> | -snmpsecuritylevel<br><i>string</i> | <p>Security level that the gateway uses for SNMPv3 messages:</p> <ul style="list-style-type: none"> <li>• AuthnoPriv—The gateway sends the username and password in encrypted format.</li> <li>• AuthPriv—The gateway transmits the SNMP traps in encrypted format.</li> <li>• noAuthnoPriv—(Default) The gateway does not encrypt the username, password, or SNMP traps.</li> </ul> <p><b>Note</b> This property is used only with SNMPv3 traps.</p>                 |
| Gate.SNMP.SecurityName<br><i>string</i>  | -snmpsecurityname<br><i>string</i>  | <p>Security name for the gateway as defined in the configuration file of the receiver. The default is netcool.</p> <p><b>Note</b> This property is used only with SNMPv3 traps.</p>                                                                                                                                                                                                                                                                                   |

| Property Name                                  | Command-Line Option                                       | Description                                                                                                                                                                                                                |
|------------------------------------------------|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gate.SNMP.SecurityAuthProtocol <i>string</i>   | <code>-snmpsecurityauthprotocol</code><br><i>string</i>   | Authentication protocol that the gateway uses: <ul style="list-style-type: none"> <li>• MD5—(Default) Message Digest 5 protocol.</li> </ul> <p><b>Note</b> This property is used only with SNMPv3 traps.</p>               |
| Gate.SNMP.SecurityPrivProtocol <i>string</i>   | <code>-snmpsecurityprivprotocol</code><br><i>string</i>   | Privacy protocol that the gateway uses to encrypt data: <ul style="list-style-type: none"> <li>• AES—Advanced Encryption Standard.</li> <li>• DES—(Default) Data Encryption Standard.</li> </ul>                           |
| Gate.SNMP.SecurityAuthPassphrase <i>string</i> | <code>-snmpsecurityauthpassphrase</code><br><i>string</i> | Password used for authentication. The default is password. <p><b>Note</b> The password must be at least eight characters long. This property is used only with SNMPv3 traps.</p>                                           |
| Gate.SNMP.SecurityPrivPassphrase <i>string</i> | <code>-snmpsecurityprivpassphrase</code><br><i>string</i> | Password used for privacy. The default is password. <p><b>Note</b> This property is used only with SNMPv3 traps.</p>                                                                                                       |
| Gate.SNMP.SNMPVersion <i>integer</i>           | <code>-snmpsnmpversion</code><br><i>integer</i>           | Version of the SNMP writer. The default is 2.                                                                                                                                                                              |
| Gate.SNMP.Specific <i>integer</i>              | <code>-snmpspecific</code><br><i>integer</i>              | Trap type value for the specific trap field in forwarded SNMP traps. The default is 1. <p><b>Note</b> This property can also be defined as @Class to forward the value of the Class column in the alerts.status table.</p> |
| Gate.SNMP.StoreAndForward <i>boolean</i>       | <code>-snmpstoreandforward</code><br><i>boolean</i>       | Whether or not the gateway runs in store-and-forward mode. The default is FALSE. <p><b>Note</b> Store-and-forward mode is not available when the gateway uses UDP.</p>                                                     |
| Gate.SNMP.StoreFile <i>string</i>              | <code>-snmpstorefile</code><br><i>string</i>              | Name and location of the storage file that the gateway uses when operating in store-and-forward mode. The default is \$OMNIHOME/var/NCO_GATE_snmp_.store.                                                                  |
| Gate.SNMP.Timeout <i>integer</i>               | <code>-snmptimeout</code><br><i>integer</i>               | Time (in seconds) that the gateway waits for a connection from an SNMP receiver before timing out. The default is 600. <p><b>Note</b> This property is used only when the Gate.SNMP.Protocol property is set to TCP.</p>   |

| Property Name                    | Command-Line Option      | Description                                                                                                                                                                                                  |
|----------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gate.SNMP.Trap<br><i>integer</i> | -snmptrap <i>integer</i> | Trap type value of the generic trap field in forwarded SNMP traps.<br><br><b>Note</b> This property can also be defined as @Severity to forward the value of the Severity column in the alerts.status table. |

## Map Definition Files

Map definition files define how the gateway maps data from the SNMP gateway to the status tables in the Fault Management database. The default map definition file is \$SOMNIHOME/gates/snmp/snmp.map.

When an event is received, it is converted to the trap format defined in the CISCO-EPM-NOTIFICATION-MIB (see the following table). All OSS clients receive the same traps in the same trap format.

**Table 22: CISCO EPM-NOTIFICATION-MIB Summary**

| Trap Name                 | Object ID                     | Type                | Value                                                                                                                                                           |
|---------------------------|-------------------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cenAlarmVersion           | 1.3.6.1.4.1.9.9.311.1.1.2.1.2 | SnmpAdmin<br>String | MIB version number, in the format <i>major version.minor version</i> .<br><br>Always set to 1.5.2.                                                              |
| cenAlarmTimestamp         | 1.3.6.1.4.1.9.9.311.1.1.2.1.3 | Timestamp           | Time when the alarm was raised.                                                                                                                                 |
| cenAlarmUpdatedTime stamp | 1.3.6.1.4.1.9.9.311.1.1.2.1.4 | Timestamp           | Alarms persist over time and their fields can change values. The updated time indicates the last time a field changed and this alarm updated.                   |
| cenAlarmInstanceID        | 1.3.6.1.4.1.9.9.311.1.1.2.1.5 | SnmpAdmin<br>String | Serial number that uniquely identifies each alarm.                                                                                                              |
| cenAlarmStatus            | 1.3.6.1.4.1.9.9.311.1.1.2.1.6 | Integer32           | Alarm status: <ul style="list-style-type: none"> <li>• 0—Not acknowledged</li> <li>• 1—Acknowledged</li> </ul>                                                  |
| cenAlarmStatusDefinition  | 1.3.6.1.4.1.9.9.311.1.1.2.1.7 | SnmpAdmin<br>String | Alarm status definition, in the format <i>integer,string</i> : <ul style="list-style-type: none"> <li>• 0,Not acknowledged</li> <li>• 1,Acknowledged</li> </ul> |
| cenAlarmType              | 1.3.6.1.4.1.9.9.311.1.1.2.1.8 | Integer             | Not used.                                                                                                                                                       |

| Trap Name                         | Object ID                      | Type                | Value                                                                                                                                                                                                                        |
|-----------------------------------|--------------------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cenAlarmCategory                  | 1.3.6.1.4.1.9.9.311.1.1.2.1.9  | Integer32           | Alarm category: <ul style="list-style-type: none"> <li>• 0—Unknown</li> <li>• 100—Raw alarm</li> <li>• 101—Root cause alarm</li> <li>• 102—Service alarm</li> </ul>                                                          |
| cenAlarmCategory Definition       | 1.3.6.1.4.1.9.9.311.1.1.2.1.10 | SnmpAdmin           | Alarm category definition, in the format <i>integer,string</i> : <ul style="list-style-type: none"> <li>• 0,Unknown</li> <li>• 100,Raw alarm</li> <li>• 101,Root cause alarm</li> <li>• 102,Service alarm</li> </ul>         |
| cenAlarmServer AddressType        | 1.3.6.1.4.1.9.9.311.1.1.2.1.11 | InetAddress<br>Type | Alarm server address type. Always set to <i>IPv4</i> .                                                                                                                                                                       |
| cenAlarmServerAddress             | 1.3.6.1.4.1.9.9.311.1.1.2.1.12 | InetAddress         | IP address of the application that sent the alarm.                                                                                                                                                                           |
| cenAlarmManaged ObjectClass       | 1.3.6.1.4.1.9.9.311.1.1.2.1.13 | SnmpAdmin<br>String | ID sent from the application to Prime Central Fault Management.                                                                                                                                                              |
| cenAlarmManaged ObjectAddressType | 1.3.6.1.4.1.9.9.311.1.1.2.1.14 | InetAddress<br>Type | Not used.                                                                                                                                                                                                                    |
| cenAlarmManaged ObjectAddress     | 1.3.6.1.4.1.9.9.311.1.1.2.1.15 | InetAddress         | IP address of the application on which the alarm occurred.                                                                                                                                                                   |
| cenAlarmDescription               | 1.3.6.1.4.1.9.9.311.1.1.2.1.16 | OctetString         | Event message text.                                                                                                                                                                                                          |
| cenAlarmSeverity                  | 1.3.6.1.4.1.9.9.311.1.1.2.1.17 | Integer32           | Integer that corresponds to the alarm severity: <ul style="list-style-type: none"> <li>• 0—Clear.</li> <li>• 1—Intermediate.</li> <li>• 2—Warning.</li> <li>• 3—Minor.</li> <li>• 4—Major.</li> <li>• 5—Critical.</li> </ul> |

| Trap Name                   | Object ID                     | Type             | Value                                                                                                                                |
|-----------------------------|-------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| cenAlarmSeverity Definition | 1.3.6.1.4.1.99.311.1.1.2.1.18 | OctetString      | String representation of the alarm severity, in the format <i>number,description</i> ; for example:<br>5,Critical                    |
| cenAlarmTriageValue         | 1.3.6.1.4.1.99.311.1.1.2.1.19 | Integer32        | Not used.                                                                                                                            |
| cenEventIDList              | 1.3.6.1.4.1.99.311.1.1.2.1.20 | OctetString      | Not used.                                                                                                                            |
| cenUserMessage1             | 1.3.6.1.4.1.99.311.1.1.2.1.21 | SnmpAdmin String | Alarm or event name; for example: <ul style="list-style-type: none"> <li>• Vm Powered Off</li> <li>• Host Connection Lost</li> </ul> |
| cenUserMessage2             | 1.3.6.1.4.1.99.311.1.1.2.1.22 | SnmpAdmin String | Service impacted by the alarm.                                                                                                       |
| cenUserMessage3             | 1.3.6.1.4.1.99.311.1.1.2.1.23 | SnmpAdmin String | Not used.                                                                                                                            |
| cenAlarmMode                | 1.3.6.1.4.1.99.311.1.1.2.1.24 | Integer          | Always set to <i>alert</i> .                                                                                                         |
| cenPartitionNumber          | 1.3.6.1.4.1.99.311.1.1.2.1.25 | Unsigned32       | Numerical ID of the service.                                                                                                         |
| cenPartitionName            | 1.3.6.1.4.1.99.311.1.1.2.1.26 | SnmpAdmin String | Service type.                                                                                                                        |
| cenCustomerIdentification   | 1.3.6.1.4.1.99.311.1.1.2.1.27 | SnmpAdmin String | Name of the customer that is impacted by the alarm.                                                                                  |
| cenCustomerRevision         | 1.3.6.1.4.1.99.311.1.1.2.1.28 | SnmpAdmin String | ID of the customer that is impacted by the alarm.                                                                                    |
| cenAlertID                  | 1.3.6.1.4.1.99.311.1.1.2.1.29 | SnmpAdmin String | Not used.                                                                                                                            |

## Gateways and DSAs Used with Prime Central

The Prime Central base application includes two application probes and one Tier 1 SNMP gateway for connection to a third-party OSS.

Prime Central requires a license to connect to and interoperate with other Cisco and third-party systems or components. The following restrictions apply:

- Prime Central Tier 1 and Tier 2 gateways may not be used to connect Prime Central to third-party systems, such as third-party trouble ticketing systems, except through a separately purchased license.

- Prime Central Tier 1 and Tier 3 data source adaptor (DSA) instances may only be used to connect to other Cisco applications or components embedded within Cisco applications, and in addition only if through a separately purchased license.
- Prime Central may not be integrated with an OSS system using an MTOSI interface except through a separately purchased license.
- Prime Central may not be integrated with Cisco applications except through a separately purchased license.

The following table lists the Tier 1 and Tier 2 gateways and the Tier 1 and Tier 3 DSAs that are available for use with Prime Central through a separately purchased license. For more information on Tier 1 gateways, see the [IBM Tivoli Netcool OMNIBus Reference Guides](#).

**Table 23: Gateways and DSAs Used with Prime Central**

| Gateway or DSA Name          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tier 1 Gateways</b>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Gateway for SNMP writer      | <p>The Gateway for SNMP Writer forwards Netcool alerts as Simple Network Management Protocol (SNMP) traps to an SNMP reader, such as the IBM Tivoli Netcool/OMNIBus SNMP probe. This allows Tivoli Netcool/OMNIBus to generate traps that are forwarded to another management platform such as SunNet Manager or HP Network Node Manager.</p> <p>The Gateway for SNMP Writer supports SNMP versions 1, 2, and 3.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/OMNIBus SNMP Writer Gateway Reference Guide</a>.</p> |
| Gateway for socket writer    | <p>The Gateway for Socket Writer uses a TCP connection to forward alerts. Any program that listens to that socket receives the alerts.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/OMNIBus Socket Writer Gateway Reference Guide</a>.</p>                                                                                                                                                                                                                                                                         |
| Gateway for flat file writer | <p>The Gateway for Flat File Writer is a unidirectional gateway that reads alerts from the Netcool/OMNIBus object server, and writes the details to a flat file. The gateway can receive insert, update, and delete notification information from multiple tables within the object server.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/OMNIBus Flat File Gateway Reference Guide</a>.</p>                                                                                                                        |
| Gateway for ODBC             | <p>The Gateway for ODBC uses a set of Open Database Connectivity (ODBC) libraries and drivers to enable data transfer between the Netcool/OMNIBus object server and Sybase, Microsoft SQL Server, Informix, DB2, and MySQL databases.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/OMNIBus Gateway for ODBC Reference Guide</a>.</p>                                                                                                                                                                               |

| Gateway or DSA Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gateway for message bus (XML/ESB)      | <p>The Gateway for Message Bus receives Netcool events from the object server, uses a transformer module to transform them to an XML format that can be understood by a destination application, and uses a transport module to send the transformed events to the application.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/OMNIBus Gateway for Message Bus Reference Guide</a>.</p>                                                                                                                                                      |
| Gateway for JDBC                       | <p>The Gateway for JDBC uses the standard Java Database Connectivity (JDBC) API to exchange alerts between Netcool/OMNIBus object servers and external databases. It communicates with the supported databases using Java Type 4 JDBC drivers supplied by the database vendors.</p> <p>The Gateway for JDBC can be used as a replacement for the Tivoli Netcool/OMNIBus Gateway for ODBC and the Tivoli Netcool/OMNIBus Gateway for Oracle.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/OMNIBus Gateway for JDBC Reference Guide</a>.</p> |
| Gateway for Oracle                     | <p>The Gateway for Oracle writes selected alert details to Oracle databases.</p> <p>The gateway writes to three Oracle database tables (status, journal, and details) to record all transactions that occur within alerts selected by an object server reader.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/OMNIBus Gateway for Oracle Reference Guide</a>.</p>                                                                                                                                                                            |
| <b>Tier 2 Gateways</b>                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Gateway for HP OpenView Service Center | <p>The Gateway for HP OpenView Service Center is a fully functional bidirectional gateway.</p> <p>Alerts forwarded from the object server go through the gateway to form HP Service Center/Service Manager incident management tickets. Both systems work together to create and update alerts and tickets.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/OMNIBus Gateway for HP OpenView Service Center/Service Manager Reference Guide</a>.</p>                                                                                           |
| Gateway for Remedy ARS                 | <p>The Gateway for Remedy ARS is a help desk system that operates on UNIX platforms. The gateway converts alerts into Remedy help desk trouble tickets. Trouble tickets are updated according to a predefined mapping throughout the lifetime of the alert.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/OMNIBus Gateway for Remedy ARS Reference Guide</a>.</p>                                                                                                                                                                           |

| Gateway or DSA Name | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gateway for TSRM    | <p>The Gateway for TSRM provides bidirectional communication between Netcool/OMNIbus and Tivoli Service Request Manager (TSRM).</p> <p>The gateway supports TSRM version 7.1 (Fix Pack 4 and later), TSRM version 7.2, and IBM Maximo Base Services (MBS) version 7.1.1.5.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/OMNIbus Gateway for TSRM Reference Guide</a>.</p> |
| <b>Tier 1 DSAs</b>  |                                                                                                                                                                                                                                                                                                                                                                                                  |
| LDAP DSA            | <p>The LDAP DSA is used to access information stored in an LDAP server.</p> <p>This type of DSA is read-only. You cannot use Netcool/Impact to insert new LDAP data into the server data store. The LDAP DSA is built in and does not require additional installation or configuration.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/Impact DSA Reference Guide</a>.</p>  |
| Socket DSA          | <p>The socket DSA provides an interface between Tivoli Netcool/Impact and a socket server.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/Impact DSA Reference Guide</a>.</p>                                                                                                                                                                                               |
| XML DSA             | <p>The XML DSA reads and extracts data from any well-formed XML document.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/Impact DSA Reference Guide</a>.</p>                                                                                                                                                                                                                |
| DB2 DSA             | <p>For more information, see the <a href="#">IBM Tivoli Netcool/Impact DSA Reference Guide</a>.</p>                                                                                                                                                                                                                                                                                              |
| Flat File DSA       |                                                                                                                                                                                                                                                                                                                                                                                                  |
| Generic SQL DSA     |                                                                                                                                                                                                                                                                                                                                                                                                  |
| HSQLDB DSA          |                                                                                                                                                                                                                                                                                                                                                                                                  |
| Informix DSA        |                                                                                                                                                                                                                                                                                                                                                                                                  |
| MS-SQL Server DSA   |                                                                                                                                                                                                                                                                                                                                                                                                  |
| MySQL DSA           |                                                                                                                                                                                                                                                                                                                                                                                                  |
| ObjectServer DSA    |                                                                                                                                                                                                                                                                                                                                                                                                  |
| ODBC DSA            |                                                                                                                                                                                                                                                                                                                                                                                                  |
| Oracle DSA          |                                                                                                                                                                                                                                                                                                                                                                                                  |
| PostgreSQL DSA      |                                                                                                                                                                                                                                                                                                                                                                                                  |
| Sybase DSA          |                                                                                                                                                                                                                                                                                                                                                                                                  |

| Gateway or DSA Name | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tier 3 DSAs</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| JMS DSA             | <p>The JMS DSA sends and receives Java Message Service (JMS) messages from within a policy.</p> <p>The JMS DSA is installed automatically when you install Netcool/Impact.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/Impact DSA Reference Guide</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Web services DSA    | <p>The web services DSA is a direct-mode DSA that Netcool/Impact automatically loads during application runtime.</p> <p>You do not have to start or stop this DSA independently of the application. The web services DSA is installed with Netcool/Impact and does not require additional installation or configuration.</p> <p>The web services DSA is compatible with its older versions in Netcool/Impact 3.x and 4.x. This means that your old IPL policies developed on Netcool/Impact 3.x and 4.x will continue to run without modification in the current version.</p> <p>The web services DSA provides support for WSDL version 1.1 and 2.0, and SOAP version 1.1.</p> <p>For more information, see the <a href="#">IBM Tivoli Netcool/Impact DSA Reference Guide</a>.</p> |



## CHAPTER 7

# Monitoring Your Data Center

This section describes how to use Prime Central to monitor your data center. It contains the following topics:

- [Introduction, on page 143](#)

## Introduction

From Prime Central's Data Center page, you can monitor the health and performance of your data center. The components that make up your data center include compute service resources (such as bare metal blade servers and virtual machines), managed VPNs, and storage devices. To access the Data Center page, choose **Assure > Services > Data Center**.

At the top of the Data Center page, you will find four tabs:

- Overview
- Compute
- Network
- Storage

The information displayed on the Data Center page will vary, depending on which of these tabs you select. A good amount of this information is gathered from Prime Performance Manager. Keep the following in mind when viewing this page:

- After Prime Performance Manager integration with Prime Central completes:
  - It will take anywhere from one hour to a few hours for Prime Performance Manager chart data to be generated and displayed.
  - All of the necessary Prime Performance Manager reports will be enabled with the correct report settings configured. For more information, see [Default Prime Performance Manager Reports, on page 144](#).
- After the Prime Central server starts, it might take a few hours for the charts for certain Data Center objects to become visible.

## Default Prime Performance Manager Reports

Take note of the reports listed in the following table. After you integrate Prime Performance Manager with Prime Central, all of these reports should be enabled within Prime Performance Manager and configured to report data for one of the four default reporting intervals (the past 15 minutes, the past hour, the past week, and the past month). We recommend that you do not make any changes to these settings because Prime Central will not display Prime Performance Manager data properly if you do so.

| Report Name                | Path                                                        | Corresponding Prime Performance Manager Dashboard Path (if applicable)                     |
|----------------------------|-------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| SNMP/Hypervisor Ping       | <b>Reports &gt; Availability</b>                            | —                                                                                          |
| Interfaces                 |                                                             |                                                                                            |
| Interface Status           |                                                             |                                                                                            |
| Interface Status Aggregate |                                                             |                                                                                            |
| CPU                        | <b>Reports &gt; Resources</b>                               |                                                                                            |
| Memory                     |                                                             |                                                                                            |
| Interface                  | <b>Reports &gt; Transport Statistics</b>                    |                                                                                            |
| Host Per Datastore         | <b>Reports &gt; Compute &gt; VMWare &gt; VMWare Cluster</b> | <b>Dashboards &gt; Compute Dashboards &gt; VMWare Dashboards &gt; VMWare Cluster Stats</b> |
| Host Total CPU             |                                                             |                                                                                            |
| Host Total Memory          |                                                             |                                                                                            |
| vCenter Host Total CPU     | <b>Reports &gt; Compute &gt; VMWare &gt; vCenter</b>        | <b>Dashboards &gt; Compute Dashboards &gt; VMWare Dashboards &gt; vCenter Host Stats</b>   |
| vCenter Host Per Network   |                                                             |                                                                                            |
| vCenter Host Per Datastore |                                                             |                                                                                            |
| vCenter Host Total Memory  |                                                             |                                                                                            |

| Report Name                | Path                                                 | Corresponding Prime Performance Manager Dashboard Path (if applicable)                             |
|----------------------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| vCenter VM Per Network     | <b>Reports &gt; Compute &gt; VMWare &gt; vCenter</b> | <b>Dashboards &gt; Compute Dashboards &gt; VMWare Dashboards &gt; vCenter VM Stats</b>             |
| vCenter VM Total Memory    |                                                      |                                                                                                    |
| vCenter VM Total CPU       |                                                      |                                                                                                    |
| vCenter VM Per Datastore   |                                                      |                                                                                                    |
| vCenter Host Per Datastore | <b>Reports &gt; Compute &gt; VMWare &gt; vCenter</b> | <b>Dashboards &gt; Compute Dashboards &gt; VMWare Dashboards &gt; vCenter Host Datastore Stats</b> |
| vCenter VM Per Datastore   | <b>Reports &gt; Compute &gt; VMWare &gt; vCenter</b> | <b>Dashboards &gt; Compute Dashboards &gt; VMWare Dashboards &gt; vCenter VM Datastore Stats</b>   |
| CPU                        | <b>Reports &gt; Resources</b>                        | <b>Dashboards &gt; Resource Dashboards &gt; CPU/Memory/Disk/Net Stats</b>                          |
| Memory                     |                                                      |                                                                                                    |
| Disk                       |                                                      |                                                                                                    |
| Interface                  | <b>Reports &gt; Transport Statistics</b>             |                                                                                                    |
| CPU                        | <b>Reports &gt; Resources</b>                        | <b>Dashboards &gt; Server Health Dashboards &gt; Server CPU/Mem/Disk/Net</b>                       |
| Memory                     |                                                      |                                                                                                    |
| Disk                       |                                                      |                                                                                                    |
| Interface                  | <b>Reports &gt; Transport Statistics</b>             |                                                                                                    |
| L3 General VPN             | <b>Reports &gt; Transport Statistics &gt; L3VPN</b>  | <b>Dashboards &gt; Transport Dashboards &gt; L3VPN Stats</b>                                       |

## Overview Window

When monitoring your data center, begin by viewing the Overview window (see the following figure). The six portlets displayed here paint a high-level picture of your data center's performance and status, providing data such as:

- An alarm count (broken down by group)
- A chart that visualizes the compute service resources that are currently running
- Tables that list the top virtual machines by four key benchmarks: memory utilization, CPU utilization, alarm count, and I/O latency

With this information, you can identify any area within your data center that needs further attention.

Figure 41: Overview Window

The screenshot displays the Cisco Prime Central interface. The top navigation bar includes Home, Design, Fulfill, Assure, Analyze, and Inventory. The main content area is titled "Data Center" and has tabs for Overview, Compute, Network, and Storage. The "Overview" tab is active, showing an "Alarms Count Summary" table and a "Top N (5): VMs with Highest Memory Utilization" table.

**Alarms Count Summary**

| Groups                 | Highest Severity | Alarm Count |
|------------------------|------------------|-------------|
| Regions                | ✓                | 0           |
| Devices                | ⚠                | 71          |
| ▶ Compute Services     | ⚠                | 18          |
| ▶ Network Services     | ✓                | 0           |
| ▶ Storage              | ✓                | 0           |
| ▶ User-Defined Static  | ⚠                | 50          |
| ▶ User-Defined Dynamic | ✓                | 0           |

2013-07-18 17:35:000 GMT

**Top N (5): VMs with Highest Memory Utilization**

| VM Name            | Host Name    | VM Manager   | Min | Max | Avg | Bar Chart   |
|--------------------|--------------|--------------|-----|-----|-----|-------------|
| Prime-R12-8GB-RHEL | sj0-i6-svr-7 | i6-vcenter-2 | 5   | 28  | 12  | ███████████ |
| PC-Dev4-8GB-80GB   | sj0-i6-svr-8 | i6-vcenter-2 | 11  | 28  | 16  | ███████████ |

© 2011-2014 Cisco Systems, Inc.

The screenshot displays the Cisco Prime Central interface. The top navigation bar includes Overview, Compute, Network, and Storage. The "Overview" tab is active, showing an "Alarms Count Summary" table and a "Resources Summary" pie chart.

**Alarms Count Summary**

Selected 0 | Total Top Level Rows 34

Show All

| Groups             | Highest Severity |
|--------------------|------------------|
| ▶ Network Services | ✓                |
| ▶ Storage          | ✓                |
| uds-ch102          | ✓                |
| uds-ch101          | ✓                |
| uds-ch101-subch1   | ✗                |
| uds-ch101-subch2   | ✓                |
| uds-ch101-subch3   | ✓                |
| uds-ch101-subch4   | ✓                |
| uds-ch101-subch15  | ✓                |

**Resources Summary**

Compute Services | OS

Bare Metal 37% (7)

Virtual Machine 67% (4)

Legend: Virtual Machine (Blue), Bare Metal (Orange)

Note the following regarding the Overview window:

- You cannot remove any of the default portlets displayed here.
- Any additional portlets you choose to add are automatically placed at the top of the window.
- You cannot customize the window's layout.

## Compute Window

From the Compute window you can view information about the compute service resources that are managed within your data center. These resources include bare metal blade servers and virtual machines, hypervisors, and device clusters. At the top of the window, you will find the following tabs:

- Compute Service
- Hypervisor
- Clusters

To view information for a particular compute service resource type, click the corresponding tab.

**Figure 42: Compute Window**

| Data Center                               |             |           |       |                   |
|-------------------------------------------|-------------|-----------|-------|-------------------|
| Overview <b>Compute</b> Network Storage   |             |           |       |                   |
| Compute Service <b>Hypervisor</b> Cluster |             |           |       |                   |
| Synchronize Add to Group                  |             |           |       |                   |
|                                           | Name        | Status    | Alarm | Total Alarm Count |
| <input type="checkbox"/>                  | prime-esxi1 | Connected | ✓     | 0                 |
| <input checked="" type="checkbox"/>       | prime-esxi2 | Connected | ⚠     | 9                 |
| <input type="checkbox"/>                  | prime-esxi3 | Connected | ✓     | 0                 |
| <input type="checkbox"/>                  | prime-esxi4 | Connected | ✓     | 0                 |
| <input type="checkbox"/>                  | prime-esxi5 | Connected | ✓     | 0                 |
| <input type="checkbox"/>                  | prime-esxi6 | Connected | ✓     | 0                 |
| <input type="checkbox"/>                  | prime-esxi7 | Connected | ✓     | 0                 |

## Compute Service Pane

From the Compute Service pane, you can view information about the bare metal blade servers and virtual machines associated with your data center.

The following table describes the information provided in the Compute Service pane.

| Column | Description                                   |
|--------|-----------------------------------------------|
| Name   | Name of a compute service resource.           |
| Status | Current status of a compute service resource. |

| Column            | Description                                                                                                                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alarm             | Indicates the highest severity of any alarms generated for the compute service resource.                                                                                                                                           |
| Total Alarm Count | Total number of alarms generated for the compute service resource.                                                                                                                                                                 |
| Server            | Server associated with the compute service resource.                                                                                                                                                                               |
| Customer          | Customer associated with the compute service resource.                                                                                                                                                                             |
| IP Address        | IP address configured for the compute service resource.                                                                                                                                                                            |
| Type              | Indicates whether the compute service resource is a bare metal blade or virtual machine.                                                                                                                                           |
| Hypervisor Type   | Type of hypervisor configured for the selected virtual machine.                                                                                                                                                                    |
| Lifecycle         | Current lifecycle state for the compute service resource: Development, Production, or Staging.<br>For more information, see <a href="#">Setting the Lifecycle State and Priority for a Compute Service Resource</a> , on page 155. |
| Priority          | Priority assigned to the compute service resource.<br>For more information, see <a href="#">Setting the Lifecycle State and Priority for a Compute Service Resource</a> , on page 155.                                             |

## Hypervisor Pane

From the Hypervisor pane, you can view information about the hypervisors associated with your data center and determine if the number of alarms for any of these hypervisors is higher than normal.

The following table describes the information provided in the Hypervisor pane.

| Column            | Description                                                                |
|-------------------|----------------------------------------------------------------------------|
| Name              | Name of a hypervisor.                                                      |
| Status            | Current status of the hypervisor.                                          |
| Alarm             | Indicates the highest severity of any alarms generated for the hypervisor. |
| Total Alarm Count | Total number of alarms generated for the hypervisor.                       |
| IP Address        | IP address configured for the hypervisor.                                  |
| VMs Count         | Number of VMs associated with the hypervisor.                              |
| Active VMs        | Number of VMs associated with the hypervisor that are currently active.    |
| Suspended VMs     | Number of VMs associated with the hypervisor that are currently suspended. |

## Cluster Pane

From the Cluster pane, you can view information about the device clusters associated with your data center and determine if the number of alarms for any of these clusters is higher than normal.

The following table describes the information provided in the Cluster pane.

| Column            | Description                                                                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name              | Name of a device cluster.                                                                                                                                                                                        |
| Host Count        | Number of host associated with the device cluster.                                                                                                                                                               |
| Alarm             | Indicates the highest severity of any alarms generated for the device cluster.                                                                                                                                   |
| Total Alarm Count | Total number of alarms generated for the device cluster.                                                                                                                                                         |
| vMotion Events    | Number of vMotion events that have occurred on the devices associated with a particular cluster.<br><br>A vMotion event is triggered each time a managed virtual machine is moved from one host to another host. |

## Network Window

From the Network window you can view information for the VPNs managed within your data center and identify any VPNs that need to be looked at more closely (as indicated by a high alarm count). The list of VPNs provided here is gathered from Prime Network.



**Note** When Virtual Routing and Forwarding (VRF) is deleted from the network, the corresponding VPN is deleted automatically after 10 days.

Figure 43: Network Window

| Service Name      | Alarm | Total Alarm Count | Site Count | Customer |
|-------------------|-------|-------------------|------------|----------|
| management        | ✓     | 0                 | 1          |          |
| TuePMG            | ✓     | 0                 | 0          |          |
| NICOLA            | ✓     | 0                 | 2          |          |
| MPLS-SP-DAY       | ✓     | 0                 | 2          |          |
| MPLS-SP-AXPO-Day1 | ✓     | 0                 | 2          |          |
| VPNX2             | ✓     | 0                 | 0          |          |
| Voice_Services    | ✓     | 0                 | 1          |          |
| O2L3VPN           | ✓     | 0                 | 0          |          |
| PMGPMG            | ✓     | 0                 | 2          |          |
| Belgacom2         | ✓     | 0                 | 3          |          |
| V176:HelloWorld1  | ✓     | 0                 | 1          |          |

The following table describes the information provided in the VPN (MPLS) pane.

| Column            | Description                                                                                                                 |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Service Name      | Name of the VPN.                                                                                                            |
| Alarm             | Indicates the highest severity of any alarms generated for the VPN.                                                         |
| Total Alarm Count | Number of alarms generated for the VPN.                                                                                     |
| Site Count        | Number of sites the VPN is associated with.                                                                                 |
| Customer          | Indicates the customer associated with the VPN. Note that only one customer can be associated with a VPN at any given time. |

## Storage Window

From the Storage window you can view information for the storage devices associated with your data center and quickly determine if you need to free up space on any of these devices. The list of devices displayed here is gathered from Prime Network.

Figure 44: Storage Window

| Name                                                                     | Type | Free Space GB (%) | Capacity GB |
|--------------------------------------------------------------------------|------|-------------------|-------------|
| <input type="checkbox"/> sjo-i6-ds2-lun9@i6-vcenter-2::sjo-i6            | VMFS | 1958.74 (96%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun8@i6-vcenter-2::sjo-i6            | VMFS | 1989.71 (97%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun7@i6-vcenter-2::sjo-i6            | VMFS | 1947.41 (95%)     | 2047.75     |
| <input checked="" type="checkbox"/> sjo-i6-ds2-lun6@i6-vcenter-2::sjo-i6 | VMFS | 2003.27 (98%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun5@i6-vcenter-2::sjo-i6            | VMFS | 1709.18 (83%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun4@i6-vcenter-2::sjo-i6            | VMFS | 1814.69 (89%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun3@i6-vcenter-2::sjo-i6            | VMFS | 1914.55 (93%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun2@i6-vcenter-2::sjo-i6            | VMFS | 1908.73 (93%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun1@i6-vcenter-2::sjo-i6            | VMFS | 1914.74 (94%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun14@i6-vcenter-2::sjo-i6           | VMFS | 967.99 (85%)      | 1135.0      |
| <input type="checkbox"/> sjo-i6-ds2-lun13@i6-vcenter-2::sjo-i6           | VMFS | 1914.74 (94%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun12@i6-vcenter-2::sjo-i6           | VMFS | 1932.47 (94%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun11@i6-vcenter-2::sjo-i6           | VMFS | 1996.33 (97%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun10@i6-vcenter-2::sjo-i6           | VMFS | 1918.77 (94%)     | 2047.75     |
| <input type="checkbox"/> sjo-i6-ds2-lun0@i6-vcenter-2::sjo-i6            | VMFS | 1033.89 (50%)     | 2047.75     |
| <input type="checkbox"/> downloads51@i6-vcenter-2::sjo-i6                | NFS  | 270.73 (35%)      | 770.95      |
| <input type="checkbox"/> datastore1@vCenter::DCDEV                       | VMFS | 23.37 (4%)        | 552.0       |
| <input type="checkbox"/> datastore1@i6-vcenter-2::sjo-i6                 | VMFS | 86.3 (99%)        | 87.25       |
| <input type="checkbox"/> datastore1 (3)@i6-vcenter-2::sjo-i6             | VMFS | 86.3 (99%)        | 87.25       |

The following table describes the information provided in the Storage window.

| Column            | Description                                     |
|-------------------|-------------------------------------------------|
| Name              | Device name.                                    |
| Type              | Device type.                                    |
| Free Space GB (%) | Percentage of available free space on a device. |
| Capacity GB       | Total storage capacity of a device.             |

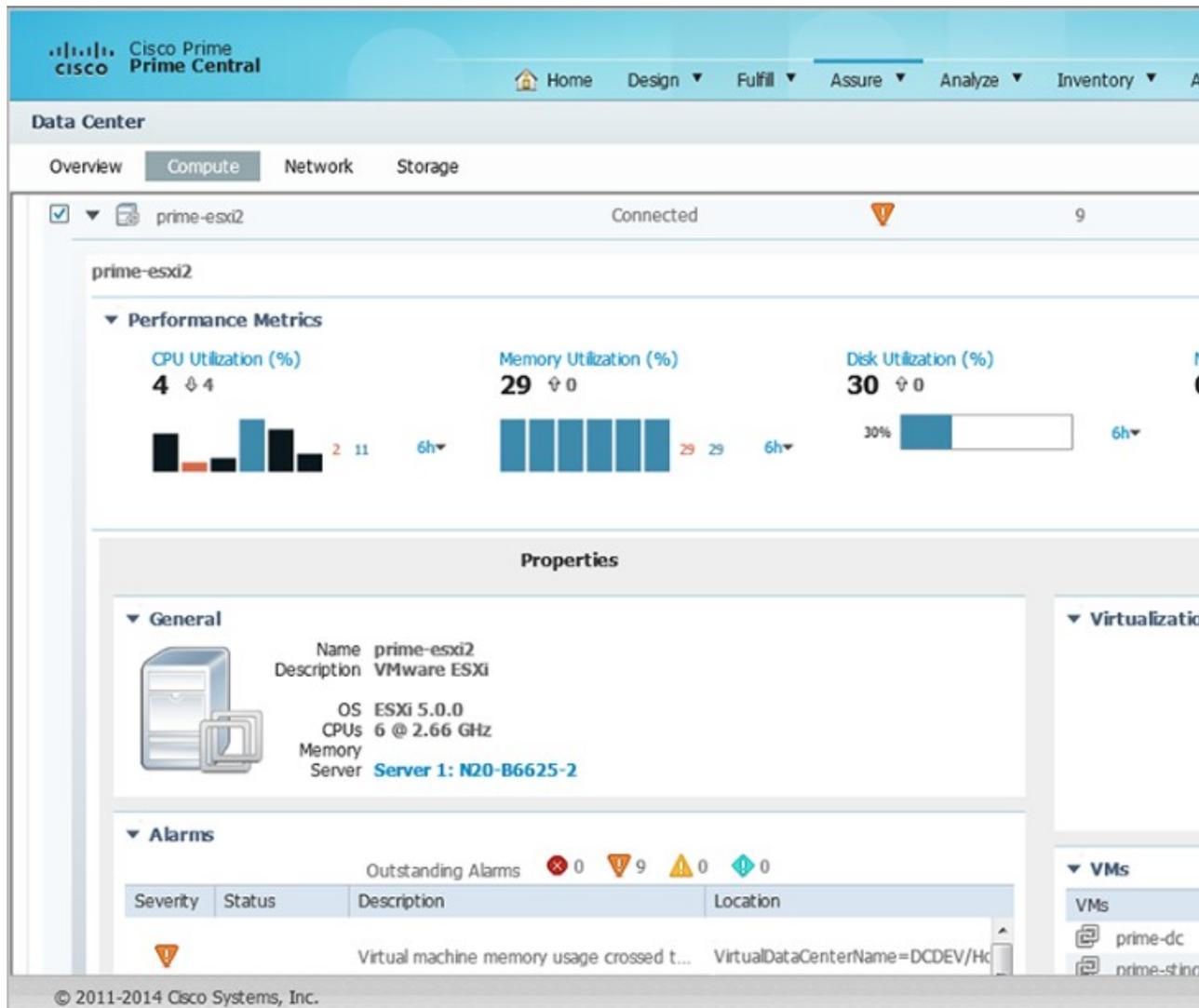
## Data Center Dashboards

When monitoring your data center, you can view dashboards that provide a higher level of detail for the selected compute service resource or VPN (see the following figure). In addition to information that is specific to the type of resource you selected (such as the number of active virtual machines running on a hypervisor or the status of physical interfaces on a VPN), these dashboards provide alarm information and performance metric charts.



**Note** The Data Center dashboard for Prime Optical devices does not include performance metric charts.

Figure 45: Data Center Dashboard



To access these dashboards:

### Procedure

- Step 1** From the Prime Central menu, choose **Assure** > **Services** > **Data Center**.
- Step 2** Do one of the following:
  - Click the **Compute** tab and proceed to Step 3.
  - Click the **Network** tab and skip ahead to Step 4.
- Step 3** Click the **Compute Service**, **Hypervisor**, or **Cluster** tab.

- Step 4** To the left of the compute service resource or VPN name, click the **Expand** icon to open the corresponding dashboard.

---

When viewing a VPN dashboard, you can cross-launch the application that manages the selected VPN or a VRF instance configured on that VPN and retrieve even more detailed information for it by clicking the appropriate source icon. Note the following:

- There are two sets of source icons. The icons in the top-right corner of the dashboard apply to the selected VPN, and the icons in the Properties table apply to the VRF selected in the VPN table.
- If multiple instances of Prime Network and Prime Optical are running and you click an icon, the instance with the highest priority associated with the VPN or VRF is launched.

In the dashboard for a bare metal server or a hypervisor, the CPUs field shows the number of CPU cores at a given CPU speed. Bare metal servers can have multiple CPU listings that might appear to be identical, but are unique per CPU.

## Data Center 360° View

To quickly view additional information for a compute service resource, VPN, or storage device, open its 360° view. To do so, place your cursor over the resource's table entry and then click the radio button in one of the following columns:

- Name column (Compute Service pane, Hypervisor pane, Clusters pane, and Storage window)
- Service Name column (Network window)
- Hypervisor Type (when launching a hypervisor's 360° view in the Compute Service pane)

The information displayed will vary (depending on the resource type you select), but typically the 360° view provides alarm information and performance metric charts. You can cross-launch the application that manages the resource and retrieve even more detailed information for it by clicking the appropriate source icon.

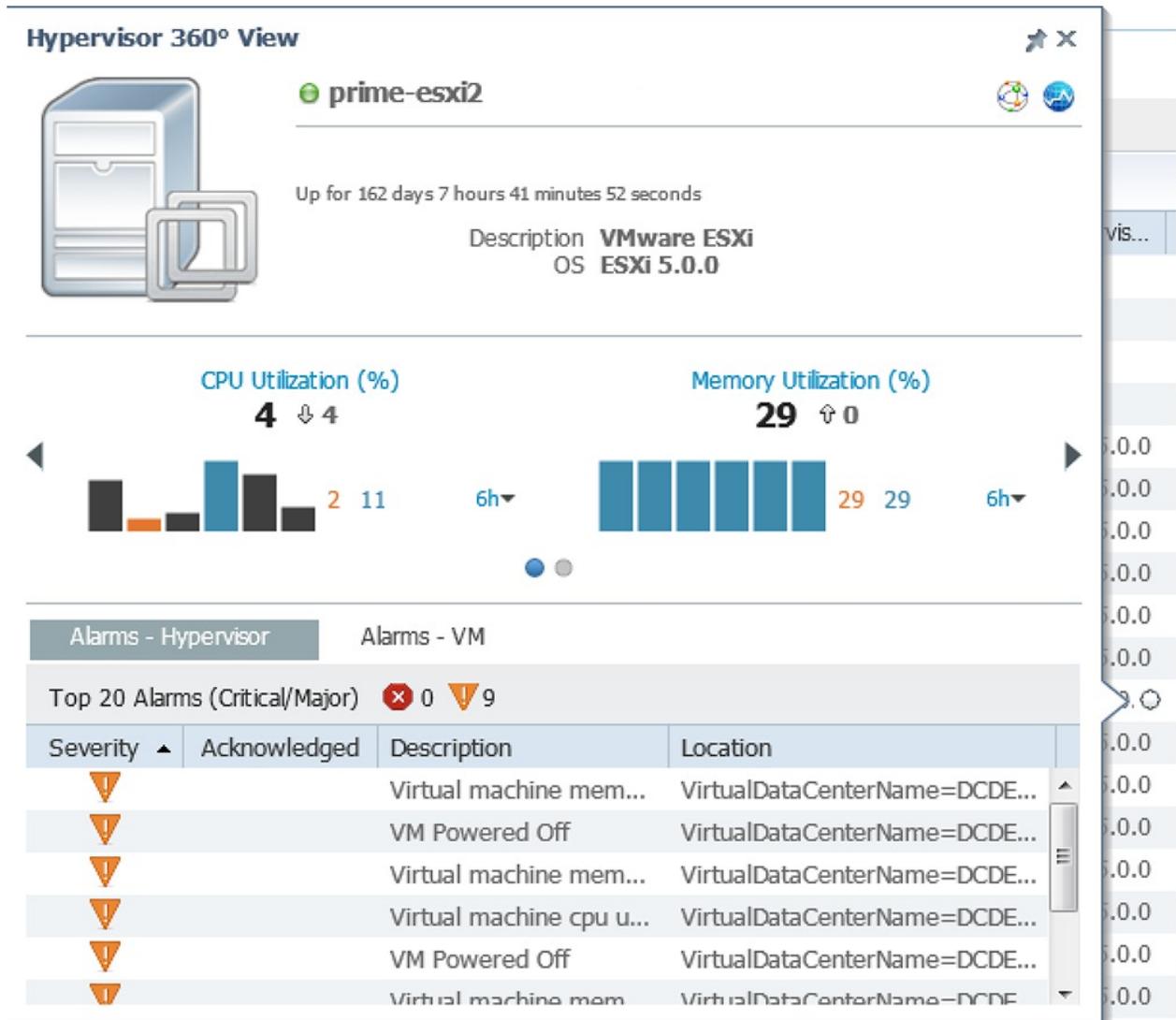


---

**Note**

- If multiple Prime Network or Prime Optical instances are running, the instance with the highest priority will be launched.
  - The 360° view for Prime Optical devices does not include performance metric charts.
-

Figure 46: Data Center 360° View



## Synchronizing Scopes and Inventory Data

Administrators can perform an on-demand, manual synchronization of user device scopes and inventory. When you first add a vCenter to Prime Network, you must manually synchronize the data center logical inventory to see the updates immediately in Prime Central. Alternately, you can wait for the automatic inventory synchronization, which occurs every two days. (Manual synchronization is not required when you add a virtual machine or ESX server to a vCenter that is already present in Prime Central.)

To synchronize scopes and inventory data:

### Procedure

- Step 1** From the Prime Central menu, choose **Assure > Services > Data Center**. The Data Center page opens.

**Step 2** Click the **Compute**, **Network**, or **Storage** tab.

**Step 3** Click the **Synchronize** icon.

**Note** Only administrators can see the Synchronize icon, which is hidden for all other users.

**Step 4** In the Synchronize dialog box, do the following:

a) Click the appropriate radio button:

- **Scopes**—Lets you synchronize device scopes for all Prime Central users.
- **Scope and Logical Inventory**—Lets you synchronize all device scope and logical inventory data.

**Note** When an application goes down, its inventory data can get out of sync with the data center. To ensure that you are viewing the latest inventory data, we recommended that you perform an on-demand synchronization with this radio button selected. We also recommend that you do this after completing the upgrade to Prime Central 1.5.2.

- **Scope and Physical Inventory**—Lets you synchronize only the device scope and physical inventory data that was received since the last synchronization.

The time stamp of the last synchronization is displayed for all of these options.

b) Click **Sync Now**.

**Step 5** In the top-right corner of the Data Center page, click the **Refresh** icon. The synchronized data is displayed.

---

## Setting the Lifecycle State and Priority for a Compute Service Resource

In the Compute Service pane, you can assign lifecycle states and priority values to resources that are associated with customers. Note that the values set for these parameters have no effect on how Prime Central manages the resources. Their purpose is to allow you to logically group resources and quickly identify the resources of a particular lifecycle state or priority when necessary. It is up to you to define what the various lifecycle states and priority values mean for your data center.

### Procedure

---

**Step 1** From the Prime Central menu, choose **Assure > Services > Data Center**.

**Step 2** From the Data Center page, click the **Compute** tab.

**Step 3** In the Compute Service pane, check the check box for the appropriate resources, and then click the **Set Lifecycle and Priority** icon.

**Step 4** Select the lifecycle state you want to assign to the resources.

**Step 5** Select the priority (P1 - P6) you want to assign to the resources.

**Step 6** Confirm that the resources you selected are listed and then click **Set**.

---

## Performing a Contextual Cross-Launch to the Common Inventory Portlet

While monitoring your data center, you can perform a contextual cross-launch to the Common Inventory portlet and view detailed inventory information for a particular blade server.

### Procedure

---

- Step 1** From the Prime Central menu, choose **Assure > Services > Data Center**. The Data Center Overview window opens.
- Step 2** Click the **Compute** tab. The Compute Service pane is displayed.
- Step 3** Do one of the following:
- To view inventory information for a particular blade server, proceed to Step 4.
  - To view inventory information for the blade server associated with a particular hypervisor, click the **Hypervisor** tab. The Hypervisor pane is displayed.
- Step 4** To the left of the appropriate blade server or hypervisor, click the **Expand** icon to open the corresponding dashboard.
- Step 5** From the General section, click the blade server's link. The Common Inventory portlet opens, displaying detailed inventory information for the selected blade server.

**Note** This link is not displayed for a hypervisor that is not associated with a blade server.

---

## Adding Data Center Resources to Groups

You can add a compute service resource, VPN, or storage device to any of the static groups configured in the Group Management portlet (**Administration > Group Management > Groups**). See [Adding a Group Member, on page 88](#).

## Associating Data Center Resources with Customers

Prime Central allows you to associate a compute service resource or VPN with a particular customer. See [Associating Resources to Customers, on page 95](#).



## APPENDIX A

# Appendix A: Troubleshooting

This appendix offers troubleshooting steps to help solve common problems while using Prime Central. Refer to the troubleshooting procedures in this appendix before contacting the Cisco Technical Assistance Center (TAC) at <http://www.cisco.com/tac>.

This section contains the following topics:

- [Troubleshooting the Prime Central Integration Layer, on page 157](#)

## Troubleshooting the Prime Central Integration Layer

Log files contain detailed information about request processing and exceptions and are your best diagnostic tool for troubleshooting the Prime Central integration layer.

Prime Central integration layer files are located in the following directory: *primeusr-home-directory/esb\_<ID>* (*~/esb\_<ID>* if you are logged in as *primeusr*).

- *servicemix.log*—Most recent log file.
- *servicemix.log.1*—Second oldest log file.
- *servicemix.log.2*—Third oldest log file.

Prime Central integration layer logger properties are located in *~/esb\_<ID>/etc/org.ops4j.pax.logging.cfg*. Useful properties include:

- *log4j.appender.out.maxFileSize=10MB*—Size of each *servicemix.log* file.
- *log4j.appender.out.maxBackupIndex=10*—Maximum number of log files. The oldest file has index 10; for example, *servicemix.log.10*.

The file also identifies the class package and log level to log; for example, *log4j.logger.com.cisco.prime=DEBUG*.

The Prime Central integration layer control script *itgctl* saves configuration and log information in *~/esb\_<ID>/diagnostics/diagnostics.[YYYYMMDDHHMMSS].tar.gz*.

**Problem** The Prime Central integration layer is not running.

**Solution** Use the ***itgctl status*** command to check the status of the Prime Central integration layer.

**Problem** The Prime Central configuration changed, but the Prime Central integration layer does not retrieve the changes.

**Solution** The Prime Central integration layer must be restarted before it can retrieve the following types of Prime Central configuration changes:

- Modifications to the applications.
- A new application registers with Prime Central.
- An existing application is removed from Prime Central.
- The Prime Central *suiteadmin* user credentials change.

Enter the following commands to restart the Prime Central integration layer:

```
itgctl stop
itgctl start
```

**Problem** An application or the Prime Central integration layer is shown as Unavailable or is missing from the Suite Monitoring or User Management portlets.

**Solution** Review the Prime Central integration layer log files for Central Authentication Service (CAS) exceptions or application connection problems. If you find CAS exceptions, enter the following commands to restart the Prime Central integration layer:

```
itgctl stop
itgctl start
```

**Problem** The Prime Central integration layer log files report any of the following problems:

- CAS unavailable
- Authentication unavailable
- Unable to establish session to domain managers

**Solution** All Prime Central components use CAS for authentication services. The CAS server runs on the Prime Central portal. If you encounter CAS problems, verify that the Prime Central portal is up and running. Then, check the connectivity between the application server and the Prime Central portal. Finally, restart the Prime Central integration layer.

**Problem** An application times out or is unavailable. The log file reports an aggregation timeout for requests.

**Solution** For the first startup, use ping or traceroute to verify routing to the application. Then, improve application performance. Finally, increase the Prime Central integration layer request aggregation timeout value.

**Problem** If you are using the User Management portlet while an application is brought up or down in Prime Central, you might receive Prime Central integration layer timeout errors.

**Solution** On the Prime Central home page, click the **Refresh Current Page** icon (see the following figure).

**Figure 47: Home Page > Refresh Current Page Icon**



**Problem** When you use the `itgctl stop` command to stop the integration layer, the following error message is generated:

```
Stop Prime Central - Integration Layer..... Warning: Karaf process can not be killed, may need to remove the process manually.. Done
```

**Solution** As the `primeusr` user, enter the following command to kill the Apache Karaf process manually:

```
ps -ef | grep karaf | grep -v grep | cut -f2 -d' ' | xargs kill -9
```

**Problem** You want to determine the role and profile associated with every integration layer instance that resides on a host.

**Solution** Enter the following command:

```
itgctl list
```

**Problem** After upgrading to Prime Central 1.5.2 and running the `itgctl status` command, Prime Central indicates that the Integration Layer's status is `UP`, even though the Suite Monitoring portlet indicates that the Integration Layer's status is `DOWN`.

**Solution** Do the following:

1. Log in to Prime Central as the root user.
2. Go to the `/etc/security` directory and open the `limits.conf` file.
3. Verify that the following values are set. If not, make the necessary changes and save the file:

- `primeusr soft nofile—51200`
- `primeusr hard nofile—65536`
- `primeusr soft nproc—204800`
- `primeusr hard nproc—204800`
- `oracle soft nproc—51200`
- `oracle hard nproc—51200`
- `oracle soft nofile—30720`
- `oracle hard nofile—65536`
- `oracle soft stack—10240`
- `hard memlock—4831838208`
- `soft memlock—4831838208`

**Problem** After upgrading to Prime Central 1.5.2, the Suite Monitoring portlet sometimes displays the integration layer's status as `Down` even though it has been started.

**Solution** The problem was observed on a server with the following applications and components installed:

- Prime Central 1.2 with a local embedded database
- Prime Central Fault Management 1.2
- Cisco Prime applications that are part of the Prime Carrier Management August 2013 release (Prime Network 4.0, Prime Optical 9.8, Prime Provisioning 6.5, and Prime Performance Manager 1.4)

After populating these applications with network data, complete the upgrade to Prime Central 1.5.2. Then, with Prime Central running, open the Suite Monitoring portlet and it indicates that the status for the integration layer, as well as the Prime applications, is `Down`.

To correct the problem, restart the integration layer by running the following commands:

- **itgetl stop**
- **itgetl start**

**Problem** In Suite Monitoring portlet, an application or the Prime Central integration layer Status is shown as `DOWN` intermittently.

**Solution** Prime Central Integration layer uses a predefined timeout period of 5 seconds for processing all the ping responses from connected DMs. If there are any network delays or resource issues, Suite Monitoring DM's status may show as `Down` for a short period.

To increase timeout value, do the following:

1. Log in as **primeusr**.
2. Uncomment **pingAggrTimeout** property in the below file and change to an appropriate value, which should be < 30000:

```
$PRIMEHOME/esb_<ID>/etc/com.cisco.prim.e.s.b.system.cfg
```

```
For example : pingAggrTimeout=25000
```

3. Uncomment **pingTimeout** property in the below files and change to an appropriate value, which should be < 30000:

```
$PRIMEHOME/esb_<ID>/etc/com.cisco.prim.e.s.b.ppm.cfg
```

```
$PRIMEHOME/esb_<ID>/etc/com.cisco.prim.e.s.b.ffusr.cfg
```

```
$PRIMEHOME/esb_<ID>/etc/com.cisco.prim.e.s.b.fmusr.cfg
```

```
$PRIMEHOME/esb_<ID>/etc/com.cisco.prim.e.s.b.agora.cfg
```

```
For example : pingTimeout=25000
```

## Troubleshooting the Prime Central Portal

The Prime Central portal features single-sign on (SSO), meaning that when you log in to the portal, you do not have to log in separately to each application within your domain.

Log files contain detailed information about request processing and exceptions and are your best diagnostic tool for SSO troubleshooting.

SSO files are located in `$XMP_HOME`, which is `primeusr-home-directory/XMP_Platform/cas.log`. The log files increment with age:

- `cas.log`—Most recent log file.
- `cas.log.1`—Second oldest log file.
- `cas.log.2`—Third oldest log file.

SSO logger properties are located in \$XMP\_HOME/tomcat-7.0.23/webapps/SSO/WEB-INF/classes/log4j.xml. Useful properties include:

```
<appender name="cas" class="org.apache.log4j.RollingFileAppender">
  <param name="File" value="cas.log" />
  <param name="MaxFileSize" value="512KB" /> - Size of each cas.log file
  <param name="MaxBackupIndex" value="3" /> - Max number of log files
</appender>

<logger name="org.jasig" additivity="true">
  <level value="ERROR" /> - File also identifies the packages of classes to log and what
  log level
  <appender-ref ref="cas" />
</logger>
```

**Problem** On Internet Explorer, portlets might spin without opening. This problem occurs occasionally when you:

- Clear your browser cache and reload the entire application.
- Log in to Prime Central immediately after clearing your browser cache.

**Solution** On the Prime Central home page, click the **Refresh Current Page** icon (refer to this [Figure 47: Home Page > Refresh Current Page Icon](#)).

**Problem** After logging in to the Prime Central portal, menu options are missing.

**Solution** Do the following:

1. Log out of the Prime Central portal.
2. Clear your browser cache.
3. Open your default browser and log back in to the Prime Central portal.

**Problem** After updating the email address or phone number in the My Account portlet, there is no confirmation message.

**Solution** Do the following:

1. From the Prime Central menu, choose **Administration > User and Privilege Management > Users**. The User Management portlet opens.
2. Refresh the page.
3. Select the user with the updated email address or phone number and click **Edit**.
4. Verify the updated email address or phone number.

**Problem** A device is missing from the Common Inventory portlet.

**Solution** Do the following:

1. Verify that all Prime Central components are operational:
  1. Log in to Prime Central and choose **Administration > System > Suite Monitoring**.
  2. In the Suite Monitoring portlet, click the **Prime Central** tab and verify that the Prime Central integration layer status is Up.
  3. Click the **Applications** tab and verify that the application status is Up.

2. Check the device inventory when logged in as the centraladmin user:
  1. Log in to Prime Central as the centraladmin user.
  2. If the Common Inventory device table shows “No data available,” and if an attempt has already been made to synchronize the inventory, skip to Step 4.
3. If the centraladmin user can see the missing device but another user cannot, you must assign device scopes or NEs to that user:
  1. See the application documentation for details:
    - Prime Network—See "Creating New Device Scopes to Control Device Access" in the [Cisco Prime Network 4.3.2 Administrator Guide](#), Chapter 6, "Controlling Device Access and Authorization Using Device Scopes."
    - Prime Optical—See "Modifying a Prime Optical User's Properties" in the [Cisco Prime Optical 10.6 User Guide](#), Chapter 8, "Managing Security."
  2. After the device scope change persists on the application, you must synchronize the scope data. In the Common Inventory device table, click the **Synchronize** icon. Click the **Scope** radio button; then, click **Sync Now**. Wait for at least 15 minutes.
4. If the device is still missing from the Common Inventory device table, verify that the device exists on the source application:
  1. Log in to Prime Central as the centraladmin user.
  2. Choose **Administration > Discovery/Adding Devices > Prime Network** or **Prime Optical**.
  3. If the device is present, verify that its status is In Service or Up and it has been discovered by the application. If the device was added recently, wait for at least 15 minutes for it to be discovered.
  4. If the device is not present, add it on the application. Wait for it to be discovered and In Service (Prime Optical) or Available/Up (Prime Network).
5. When the device is discovered by the individual applications, synchronize the device inventory:
  1. Log in to Prime Central as the centraladmin user.
  2. In the Common Inventory device table, click the **Synchronize** icon.
  3. Click the **Inventory and Scope** radio button.
  4. Click **Sync Now**.
6. If the device is still missing from the Common Inventory portlet:
  1. Enter the following command to log in to the Prime Central shell:
 

```
ssh -l primeusr prime-central-server
```
  2. Change directories to the \$XMP\_HOME directory and enter the following commands:
 

```
tar -czvf common_inv_logs.tar.gz common_inventory.log
/opt/primecentral/apache-servicemix-4.4.1-fuse-00-08/data/log/servicemix.log
```
  3. Send the log files to the Cisco TAC.

**Problem** If you are using Internet Explorer, when you zoom in or out to less than or greater than 100% screen resolution, the User Management and Common Inventory filters become blurry. This problem occurs only when you use the Filter option; no other views in either portlet blur when you zoom in or out.

**Solution** In Internet Explorer, do not zoom in or out when filtering data in the User Management and Common Inventory portlets. Alternately, use Firefox to launch Prime Central.

**Problem** In the My Account portlet and Add User wizard, if you change your password to include a trailing space at the end, Prime Central removes the last space character automatically. The next time you log in to Prime Central with the password that includes the trailing space, your password is denied.

**Solution** When creating a password, do not include a trailing space at the end.

**Problem** After you log in to the Prime Central portal, the login progress icon spins indefinitely or you see the “CAS is Unavailable” error message.

**Solution** Restart the Prime Central portal.

**Problem** After adding a QvPC device in Prime Network, if you are unable to view associated Virtual Machine, Hypervisor Data for the virtual cards of this device in Prime Central Common Inventory portlet.

**Solution** Do the following:

1. From the Prime Central menu, choose **Assure > Services > Data Center**. The Data Center page opens.
2. Click the **Compute, Network, or Storage** tab.
3. Click the **Synchronize** icon.



---

**Note** Only administrators can see the Synchronize icon, which is hidden for all other users.

---

4. In the Synchronize dialog box, do the following:
  1. Click the **Scope and Logical Inventory** radio button.
  2. Click **Sync Now**.
5. In the Common Inventory device table, click the **Synchronize** icon. Click the **Scopes and Inventory** radio button; click **Synchronize all data** radio button, then, click **Sync Now**. Wait for the Synchronization to complete.

## Troubleshooting Prime Central Security

**Problem** False positives are indicated during a scan for security vulnerabilities.

**Solution** Prime Central components communicate over a highly secure message bus using the secure socket layer (SSL), a strong encryption algorithm, and two-way, certificate-based authentication. We recommend that you work with Cisco TAC to verify whether any found issues require further attention.

## Troubleshooting Prime Network

**Problem** After registering with Prime Central, Prime Network is shown in the Suite Monitoring portlet > Applications tab, but its state is Down.

**Solution** Do the following:

1. Verify that the Prime Central integration layer configuration has been generated for Prime Network. Make sure the `com.cisco.prime.esb.ana.cfg` file has valid values for `anaComURI` and `anaPtpServer`.
2. Verify that the Prime Network gateway is up and accepting connections (BQL).
3. Check the `servicemix.log` file and capture any `ana-bnd` exceptions.
4. To bypass CAS authentication, configure `anaPtpUser` and `anaPtpPw` in `com.cisco.prime.esb.ana.cfg`.
5. Look for deserialization errors caused by a version mismatch between Prime Network and the Prime Central integration layer.
6. To troubleshoot transformation issues, look for the JMS queue name in the format `DM_operation-name_net://net:XXX`.

## Troubleshooting Prime Optical

**Problem** After registering with Prime Central, Prime Optical is not shown in the Suite Monitoring portlet > Applications tab.

**Solution** Do the following:

1. Check the `DMIntegrator.log` file to see if the Prime Optical registration failed or succeeded.
2. Check if an incorrect hostname was entered for the Prime Central database during the Prime Optical registration. In the `DMIntegrator.log` file, check the value of the `[SERVER:]` property, which should be the hostname of the server where the Prime Optical database is installed.

**Problem** After registering with Prime Central, Prime Optical is shown in the Suite Monitoring portlet > Applications tab, but its state is Down.

**Solution** Do the following:

1. If the Prime Optical server did not start, log in to the Prime Optical workstation as the root user and enter the `opticalctl status` command. The output should show the CTM Server, SMSService, and CORBAGWService services. If those services are not running, enter the `opticalctl start` command to start them.
2. As the `primeusr` UNIX OS user, log in to the Prime Central workstation and enter the `itgctl restart` command to reconfigure the Prime Central integration layer.
3. Wait for some time; then, check if the Prime Optical state changes to Up in the Suite Monitoring portlet > Applications tab.

If the problem persists, do the following:

1. Verify that the Prime Central integration layer configuration has been generated for Prime Optical. In the `com.cisco.prime.esb.ctm.cfg` file, make sure the file has valid values for `ctmComURI` and `ctmCorbaServer`. If not, restart the Prime Central integration layer to configure Prime Optical.
2. On the Prime Optical server, enter the command `showctm -v` to see if the CORBAGWService is up.
3. Check the `servicemix.log` file and capture any `ctm-bnd` exceptions. If you see CAS exceptions, verify that the Prime Central portal is up and running. Then, check the connectivity between the application server and the Prime Central portal. Finally, restart the Prime Central integration layer.

4. See the [Cisco Prime Optical 10.6 User Guide](#) to create the GateWay/CORBA User on Prime Optical. Use `ctmCorbaUser=gateway-corba-user` and `ctmCorbaPw=gateway-corba-user-password` in the `com.cisco.prime.esb.ctm.cfg` file. Restart the Prime Central integration layer.

**Problem** Prime Optical is shown as Up in the Suite Monitoring portlet > Applications tab, but the menu options to launch Prime Optical are missing.

**Solution** Do the following:

1. In the User Management portlet, check whether the user has Prime Optical in his application access privileges.
2. If necessary, edit the user and check the **Grant Access to Prime Optical** check box in the Application Access Privilege screen.

**Problem** Cannot cross-launch Prime Optical from Prime Central.

**Solution** Do the following:

1. Verify that the Prime Optical server is up and running. As the root user, log in to the Prime Optical workstation and enter the `opticalctl status` command. The output should show the CTM Server, SMService, and Apache Web Server services, which are required to cross-launch Prime Optical from Prime Central.
2. The Prime Optical client is launched through Oracle Java Web Start technology. Verify that JRE 1.6 is installed on the client workstation, and that JNLP files are opened with Java Web Start.
3. When the Prime Optical client is launched for the first time on the client workstation, the client is downloaded, installed, and launched. Consequently, the first launch might take several minutes. If the client launches too slowly, the first opening might fail. Retry the cross-launch.
4. If the client is downloaded and launched, but closes without any messages, collect the `Cisco/PrimeOptical_96/debug/CTMC-debug*.log` files from the client workstation and contact the Cisco TAC.

**Problem** You receive an “Unable to connect” error when you try to cross-launch Prime Optical from the Prime Central portal or from Prime Network Vision.

**Solution** Send an update command through the browser by entering the following URL:

```
http://portal-server:portal-http-port/cx1/jnlpupdate?dm=COM-URI
```

where:

- `portal-server` is the hostname of the Prime Central portal host.
- `portal-http-port` is the portal port number.
- `COM-URI` is the Prime Optical identifier and can be found in the Prime Central Suite Monitoring portlet.

For example, if the Prime Central portal is running on the “prime\_portal” host on port 8443 and the identifier for Prime Optical is 4, enter:

```
http://prime_portal:8443/cx1/jnlpupdate?dm=opt://opt:4
```

## Troubleshooting Prime Performance Manager

**Problem** After registering with Prime Central, Prime Performance Manager is not shown in the Suite Monitoring portlet > Applications tab.

**Solution** Do the following:

1. On the Prime Performance Manager server, check the `/opt/CSCOppm-gw/prime-integrator/DMIntegrator.log` file to see if the Prime Performance Manager registration failed or succeeded.
2. Check if an incorrect hostname was entered for the Prime Central database during the Prime Performance Manager registration. In the `DMIntegrator.log` file, check the value of the `[SERVER:]` property, which should be the hostname of the server where the Prime Central database is installed.
3. If incorrect Prime Central database information was entered, re-enter the `/opt/CSCOppm-gw/bin/ppm primecentralintegration` command on the Prime Performance Manager gateway server. Use the correct database information.
4. If a previous incorrect instance of Prime Performance Manager exists in the Suite Monitoring portlet, do the following:
  1. In the Suite Monitoring portlet, click the **Applications** tab.
  2. Click the **Prime Performance Manager** radio button.
  3. Click **Delete**.
  4. After Prime Performance Manager has been removed from Prime Central, enter the `/opt/CSCOppm-gw/bin/ppm primecentralintegration` command on the Prime Performance Manager gateway server.

**Problem** After registering with Prime Central, Prime Performance Manager is shown in the Suite Monitoring portlet > Applications tab, but its state is Down.

**Solution** Do the following:

1. Restart Prime Performance Manager to complete the Prime Central registration. As the root user, log in to the Prime Performance Manager gateway server and enter the `/opt/CSCOppm-gw/bin/ppm restart` command. Log in to the Prime Performance Manager unit workstations and enter the `/opt/CSCOppm-unit/bin/ppm restart` command. Enter the `ppm status` command to check the operational status of Prime Performance Manager.
2. As the primeusr UNIX OS user, log in to the Prime Central workstation and enter the `itgctl restart` command to reconfigure the Prime Central integration layer.
3. Wait for some time; then, check if the Prime Performance Manager state changes to Up in the Suite Monitoring portlet > Applications tab.

**Problem** Prime Performance Manager is shown as Up in the Suite Monitoring portlet > Applications tab, but the menu options to launch Prime Performance Manager are missing.

**Solution** Do the following:

1. In the User Management portlet, check whether the user has Prime Performance Manager in the application access privileges.

2. If necessary, edit the user and check the **Grant Access to Prime Performance Manager** check box in the Application Access Privilege area.

**Problem** Cannot cross-launch Prime Performance Manager from Prime Central.

**Solution** Do the following:

1. Verify that the Prime Performance Manager gateway server is up and running. As the root user, log in to the Prime Performance Manager server and enter the **ppm status** command. All services should be running. If not, enter the **ppm restart** command to restart Prime Performance Manager.
2. If the problem persists, enter the **ppm tac** command on the Prime Performance Manager gateway server to collect the debug files. Then, contact the Cisco TAC.

## Troubleshooting Prime Provisioning

**Problem** After logging in to Prime Central, if you click the **Add Portlets** icon and add the Device SR Count or SR Summary portlets, a Prime Provisioning login screen might appear. Because you are already logged in to Prime Central, you should not be prompted to log in a second time.

**Solution** This problem occurs when a user does not have the Application Access Privilege set to Prime Provisioning. The user can click the Add Portlets icon and add the Device SR Count or SR Summary portlets, at which point the Prime Provisioning login screen appears.

To give the user access to Prime Provisioning, do the following:

1. From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
2. In the User Management portlet, select the user that you want to edit and click **Edit**.
3. In the Enter User Info screen, click **Next**.
4. In the Application Access Privilege area, make sure the **Grant Access to Prime Provisioning** check box is checked. Click **Next**.
5. In the Assign Groups & Group Roles screen, click **Next**.
6. In the Assign Additional Individual User Roles screen > Prime Central tab, make sure the **Administrator** check box is checked. In the Prime Provisioning tab, click the desired radio button. Click **Next**.
7. In the Summary screen, click **Finished**. The updated user is displayed in the Users tab. When that user opens the Device SR Count or SR Summary portlets, he is not prompted to log in a second time.

**Problem** After registering with Prime Central, Prime Provisioning is shown in the Suite Monitoring portlet > Applications tab, but its state is Down.

**Solution** Do the following:

1. Use the **./prime.sh** command to check the list of running servers and verify that all services have started:

| Name     | State   | Gen | Exec Time           | Success | Missed |
|----------|---------|-----|---------------------|---------|--------|
| nspoller | started | 1   | Dec 16 01:55:08 EST | 817     | 0      |
| dbpoller | started | 1   | Dec 16 01:55:08 EST | 824     | 0      |
| httpd    | started | 1   | Dec 16 01:55:13 EST | 829     | 0      |
| rgserver | started | 1   | Dec 16 01:55:58 EST | 817     | 0      |
| cnserver | started | 1   | Dec 16 01:55:13 EST | 823     | 0      |

2. If some services have stopped, enter the following commands to stop and restart them:

```
./prime.sh stopall
```

```
./prime.sh start
```

3. If the problem persists, check the log file in *Prime-Provisioning-installation-directory*/tmp.

## Troubleshooting Prime Fault Management

**Problem** The Alarm Browser portlet displays the error “The application failed to run.”

**Solution** To open the Alarm Browser portlet, you must accept the self-signed, untrusted security certificates. In the Warning - Security dialog box, if you click **No** to the following message, the security certificate is denied, and the Alarm Browser displays the error “The application failed to run”:

```
This web site's certificate cannot be verified. Do you want to continue?
```

Depending on your browser, do one of the following to resolve the error:

### Mozilla Firefox

1. Log out of the Prime Central portal.
2. Clear your browser cache.
3. Choose **Tools** > **Options** and click the **Advanced** panel.
4. Click the **Encryption** tab.
5. Click **View Certificates**. The Certificate Manager dialog box opens.
6. Click the **Servers** tab and delete the certificate for the Fault Management server (with port 16311).
7. At the confirmation prompt, click **OK**.
8. Click **OK** to close the Certificate Manager dialog box.

### Microsoft Internet Explorer

1. Log out of the Prime Central portal.
2. Log back in to the Prime Central portal and accept the self-signed, untrusted security certificates.

**Problem** The Alarm Browser does not show alarms for a supported application, even though the application is shown as Up in the Suite Monitoring portlet > Applications tab.

**Solution** If an application is registered with Prime Central but is not up and running when Prime Central Fault Management is installed, you must manually register with the application if you want to receive alarms immediately. (Within 10 minutes of the Prime Central Fault Management installation, an automatic cron job starts alarm retrieval.)

To bypass the 10-minute waiting period and begin receiving alarms immediately, do the following:

1. As the primeusr user, log in to the Prime Central Fault Management server.
2. After the application is registered with Prime Central, go to the *installation-directory*/prime\_integrator/scripts folder and enter:

```
./DMRegistration.sh
```

**Problem** The Alarm Browser does not show alarms for Prime Performance Manager, even though the application is shown as Up in the Suite Monitoring portlet > Applications tab.

**Solution** If Prime Performance Manager is supposed to send alarms directly to Prime Central Fault Management, make sure an upstream OSS host is configured correctly in the Prime Performance Manager System Event Editor. The OSS host must be a fully qualified hostname or an IP address.

**Problem** The Alarm Report portlet generates an error when you open the following predefined reports:

- Events Details
- Performance Details

**Solution** By default, Prime Central Fault Management is configured to support detailed alarm reports for 50,000 alarms. For reports with more than 50,000 alarms, you can reduce the elapsed period and run multiple reports on a smaller subset of alarms. Alternately, you can increase the Java heap size of the reporting server to 3 GB and run detailed alarm reports for up to 100,000 alarms.

To increase the Java heap size on the reporting server:

1. As the primeusr user, log in to the Prime Central Fault Management server.
2. Enter the following command to stop the Fault Management server:  
**\$NCHOME/fmctl stop**
3. Change directories to  
**\$NCHOME/tipv2/profiles/TIPProfile/config/cells/TIPCell/nodes/TIPNode/servers/server1.**
4. Use a standard text editor such as vi to open the server.xml file and change the maximumHeapSize value to **3072**.




---

**Note** If you have set up disaster recovery on another device, you must also make this change on that device.

---

5. Save and close the server.xml file.
6. Enter the following commands to start the Fault Management server:

```
su - primeusr  
fmctl start
```

**Problem** After generating a report while using the Alarm Report portlet and either logging out of Prime Central or closing the portlet, you may receive the following Authentication Required prompt:

A username and password are being requested by `https://server-name:port-number`. The site says: "Cognos 8."

You are prompted to enter a username and password.

**Solution** At the Authentication Required prompt, click **Cancel**.

**Problem** In the Suite Monitoring portlet > Prime Central tab, the Prime Central Fault Management state is Down.

This problem occurs when Prime Central and the Fault Management component are installed on the same server with an embedded Oracle database, and the server is rebooted. The Oracle database takes longer to

restart automatically than does Fault Management. Because Fault Management cannot connect to the Oracle database, its state is shown as Down.

**Solution** As the `primeusr` user, restart Prime Central Fault Management:

**fmctl stop**

**fmctl start**

**Problem** After performing any of the following alarm management operations, the Alarm Browser does not display the result:

- Acknowledging or deacknowledging an alarm
- Clearing an alarm
- Retiring an alarm
- Adding notes to an alarm

**Solution** In the Alarm Browser portlet, click the **Refresh** icon. If the result is still not displayed after a manual refresh, do the following:

1. Open the Message Center.
2. Find the alarm action and click the **Memo** field to view any error information. (Errors reported by the applications prevent Prime Central Fault Management from completing the alarm action.)
3. If you see any timeout errors, verify that the Prime Central server and the application are synchronized.
4. If an error indicates that the alarm no longer exists on the application, do the following:
  - If the alarm state is Cleared, wait up to one hour for the alarm to be removed automatically.
  - If the alarm state is not Cleared, resynchronize the alarms by opening an SSH session on the Prime Central Fault Management server and entering:

**su – primeusr**

**fmctl resync**

**Problem** Notes added via the NBI Alarm Management API for Prime Network appear twice in the Prime Central Fault Management Alarm Browser.

**Solution** Make sure that the `username` element in the NBI call specifies a valid Prime Central Fault Management user. If an invalid user is specified, or the `username` element is left empty, a duplicate note is created for the alarm.

**Problem** `centraladmin` is indicated as the relevant user for notes added via the NBI Alarm Management API, even though a different username was specified.

**Solution** Make sure that the `username` element in the NBI call specifies a valid Prime Central Fault Management user. If an invalid user is specified, `centraladmin` is used instead.

**Problem** Suite Monitoring portlet indicates that Fault Management's status is `Down` (applicable to Fault Management 1.2 and later).

**Solution** If the Suite Monitoring portlet indicates that the integration layer is also down, begin by troubleshooting why. As soon as the integration layer becomes operational, Fault Management should as well.

If Fault Management continues to be down, even after the integration layer comes up, first check the integration layer's log file to determine if there are any network connection issues between the integration layer and the Fault Management server. If there are no connection issues, you then need to determine which Fault Management components are not running. The Suite Monitoring portlet sends a status request to Fault Management. At this point, Fault Management checks if all of its components are running. If they are, then the portlet indicates that the integration layer's status is Up.

The Suite Monitoring portlet's status check is equivalent to running the `fmctl status` command as *primeusr* on the Fault Management server. If you run this command on the Fault Management server and it returns:

- **SUCCESS:** Prime Central Fault Management is fully started, then Fault Management is up and running. Recheck the integration layer log files for more troubleshooting hints.
- **WARNING:** Prime Central Fault Management is in an indeterminate state, then Fault Management is still down. You will need to determine which components are down and then review the appropriate log files for more details:
  - ObjectServer: `~/faultmgmt/omnibus/log/NCOMS.log`
  - Oracle Gateway: `~/faultmgmt/omnibus/log/nco_g_oracle.log`
  - SNMP Probe: `~/faultmgmt/omnibus/log/mtrtpd.log`
  - CORBA Probe: `~/faultmgmt/omnibus/log/cisco_ctm_corba_v9_idXX.log`
  - TIP/TCR: `~/faultmgmt/tipv2/profiles/TIPProfile/logs/server1/SystemOut.log`
  - Impact: `~/faultmgmt/log/netcool-errors.log`
  - DMRegistration: `~/faultmgmt/log/dmregistration.log`

To restart Fault Management, run the **fmctl restart** command.

To view more detailed information, run the **fmctl** command.

**Problem** The Fault Management Oracle gateway is down and does not come up after restart.

**Solution** The problem is caused by one of two things:

Prime Central is installed on the same server as Fault Management and the Oracle database came up after the Oracle gateway. Restart the gateway by entering the following commands:

- **su - primeusr**
- **nco\_g\_oracle &**

The gateway database may have become corrupt. Do the following:

- Stop the gateway:
  - **kill -9 <nco\_g\_oracle pid>**
- Move the contents of the `~/SOMNIHOME/var/nco_g_oracle` directory to the `/tmp/nco_g_oracle` directory.
- Restart the gateway:
  - **su - primeusr**
  - **nco\_g\_oracle &**

**Problem** You see `mbind: Invalid Argument` errors in the Fault Management log files.

**Solution** Do the following:

1. Remove the `numactl-devel` Red Hat RPM package:
  1. Log in as the root user.
  2. Enter:
 

```
rpm -ev numactl-devel
```
2. Remove all instances of the `mbind: Invalid Argument` error in the following files:
  - `~/faultmgmt/impact/etc/NCI_ReportsHSQLDB.ds`
  - `~/faultmgmt/impact/etc/NCI_defaultobjectserver.ds`
  - `~/faultmgmt/impact/etc/NCI_wsadmin.props`

**Problem** Retired alarms are not deleted from the Oracle database after 14 days.

**Solution** Do one of the following:

If the `/tmp/fm_backups-date.tar` file exists:

1. Log in as the root user.
2. Enter the following commands:
 

```
# mkdir /tmp/fm
# cp /tmp/fm_backups*.tar /tmp/fm
# cd /tmp/fm
# tar -xvf fm_backups*.tar
# cp tmp/FaultMgmtCron.csh /etc/cron.hourly
# chmod 777 /etc/cron.hourly/FaultMgmtCron.csh
# rm -rf /tmp/fm
```

If the `/tmp/fm_backups-date.tar` file does not exist:

1. Log in as the root user.
2. Enter:
 

```
vi /etc/cron.hourly/FaultMgmtCron.csh
```
3. Copy and paste the following text into the `FaultMgmtCron.csh` file. If your `primeusr` home folder is not `/opt/primecentral`, make the appropriate changes.

```
#!/usr/bin/env tcsh

echo Current directory is 'pwd'
set PRIMEHOME=/opt/primecentral
set PRIMEFMHOME=/opt/primecentral/faultmgmt
source /opt/primecentral/.cshrc

cd /opt/primecentral/faultmgmt/prime_integrator/scripts
./AlarmPartitioning.sh
```

4. Save the file.

5. Enter:

```
chmod 777 /etc/cron.hourly/FaultMgmtCron.csh
```





## INDEX

### A

- AAA authentication [53](#)
- adding [8, 24, 37, 41, 43, 92](#)
  - customers [92](#)
  - groups [37](#)
  - portlets [8](#)
  - privileges [43](#)
  - roles [41](#)
  - users [24](#)
- Alarm Report portlet, using [125](#)
- alarms [109, 111, 112, 113](#)
  - acknowledging/deacknowledging [111](#)
  - adding notes [113](#)
  - clearing [112](#)
  - retiring [112](#)
  - viewing a summary of [109](#)
- audience [xi](#)
  - intended [xi](#)

### C

- Cisco InTracer [14](#)
- common inventory, viewing [70, 71](#)
- customers [93, 94, 95, 97](#)
  - associating resources to [95](#)
  - deleting [95](#)
  - editing [94](#)
  - exporting data [97](#)
  - quick view [93](#)
  - removing resources from [97](#)
- customizing [5, 7](#)
  - login advisory messages [5](#)
  - portal [7](#)

### D

- data [19](#)
  - exporting [19](#)
- data center [154](#)
  - synchronizing scopes and inventory data [154](#)
- device scopes, assigning [26](#)
- device scopes, reassigning [30](#)
- documentation, related [xi](#)

### E

- exporting [84](#)
  - inventory data [84](#)
- external authentication, configuring [51](#)

### F

- fault management [99, 100](#)
  - alarm processing [100](#)
  - overview [99](#)
- filtering [16, 17](#)
  - advanced filter [17](#)
  - quick filter [16](#)

### G

- groups [37, 38](#)
  - deleting [38](#)
  - editing [37](#)

### H

- home page [10](#)
  - changing the layout [10](#)

### I

- inventory [72, 73, 76](#)
  - synchronizing data [72](#)
  - viewing details [76](#)
  - viewing physical inventory [73](#)

### K

- key features [2](#)

### L

- logging [4, 20](#)
  - in [4](#)
  - out [20](#)

**M**

- monitoring [57, 58, 60, 64](#)
  - domain managers [58](#)
  - Prime Central [57](#)
  - quick view [60](#)
  - service requests [64](#)

**O**

- obtaining documentation [xii](#)

**P**

- passwords, changing [32](#)
- portal [12](#)
  - menu structure [12](#)
- portlets [9, 10, 23, 32, 57, 64, 65, 69, 102](#)
  - Alarm Browser [102](#)
  - Common Inventory [69](#)
  - Device SR Count [64](#)
  - maximizing or minimizing [9](#)
  - My Account [32](#)
  - removing [9](#)
  - SR Summary [65](#)
  - Suite Monitoring [57](#)
  - User Management [23](#)
  - User Preferences [10](#)
- Prime Central version, viewing [19](#)
- privileges [44](#)
  - deleting [44](#)
  - editing [44](#)

**R**

- reports [129, 130, 131, 132](#)
  - creating [129](#)
  - deleting [132](#)
  - saving or emailing [130](#)
  - scheduling [129](#)

- reports (*continued*)
  - setting properties [131](#)
  - specifying the order [131](#)
- roles [41](#)
  - deleting [41](#)
  - editing [41](#)

**S**

- security [3, 50](#)
  - audit information [50](#)
  - features [3](#)
- session timeout, changing [11](#)
- sorting data [19](#)
- submitting a service request [xii](#)

**T**

- time zone, changing [10](#)
- troubleshooting [157, 160](#)
  - Prime Central integration layer [157](#)
  - Prime Central portal [160](#)

**U**

- user accounts, supported [7](#)
- user security settings [34, 35](#)
  - configuring [34](#)
  - descriptions [35](#)
- users [28, 29, 31, 32, 34, 44, 46, 47, 48, 49, 50](#)
  - bulk import [44, 46, 47](#)
  - bulk login reporting [48](#)
  - copying [31](#)
  - deleting [32](#)
  - editing [29](#)
  - enabling [34](#)
  - exporting data [49](#)
  - external authentication [50](#)
  - quick view [28](#)