
# Setting Up Prime Network and Using Prime Network with Cisco Prime Central

These topics introduce you to the Prime Network Administration GUI client and describe the setup tasks you should perform after installing Prime Network. These tasks configure Prime Network so that other users can log into the GUI clients and use Prime Network to manage the NEs and network.



## Setting Up and Launching the Prime Network Administration GUI Client

**Note** If Prime Network is installed with Cisco Prime Central, users can log into Prime Network Administration by clicking the **Administration** tab in the Cisco Prime Portal. If a user tries to log into a Prime Network standalone or Webstart client, they will be redirected to the Cisco Prime Portal. For more information about using Prime Network with Cisco Prime Central, refer to the *Cisco Prime Network 4.2 User Guide*.

These topics explain how to customize and launch the Administration client:

- Extending Prime Network and Its Clients, page 1-3

### Launching the Administration Client

Prime Network Administration is password-protected to ensure security and is available only to users with Administrator privileges. You can use the Prime Network Administration GUI client to configure a variety of global GUI client properties, such as requiring that passwords be changed on a regular basis, disabling accounts after long periods of inactivity, and locking accounts after repeated unsuccessful login retries. These properties are applied to all of the Prime Network GUI clients, such as Prime Network Vision and Prime Network Events. Only a *root* user account created when you install Prime Network. The root user can then create accounts for other users. The settings in individual user accounts specify the GUI tasks the user can perform.

**Note** Users must have Administrator privileges to use the Administration GUI client. All of the procedures described in this guide require Administrator privileges unless otherwise noted.

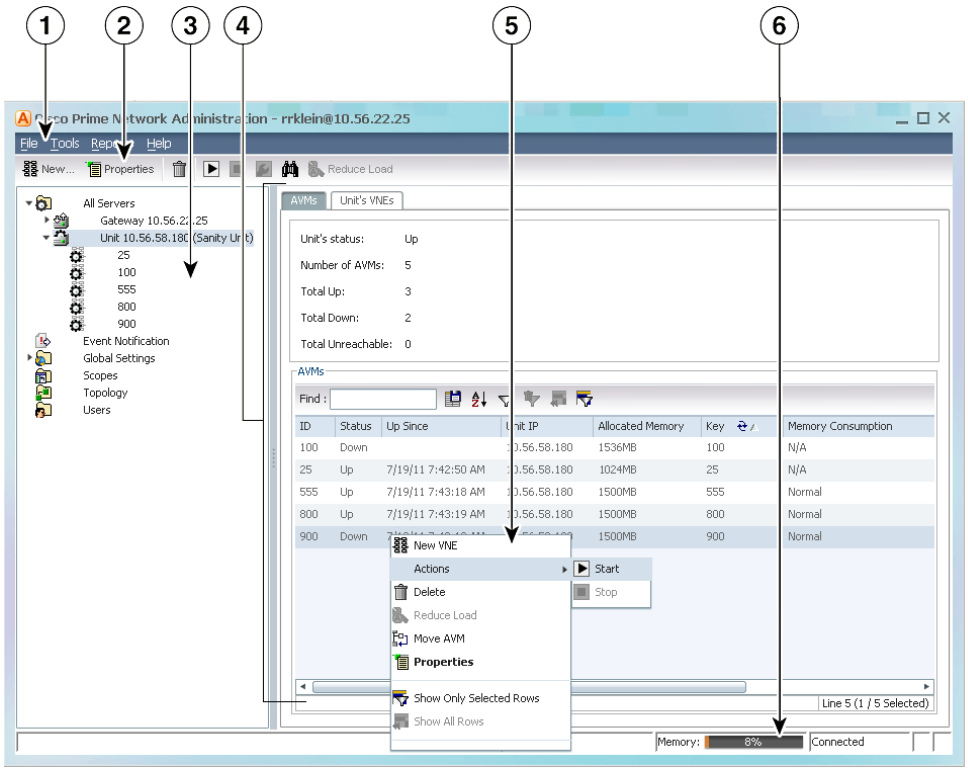
When you log out of the Administration GUI client, any changes you made are automatically saved, including changes to VNEs. Some changes may require a restart of the AVMs or VNEs, or event the Prime Network gateway. These requirements are noted with the relevant procedures.

Instructions for downloading and installing GUI clients are provided in the *Cisco Prime Network 4.2 Installation Guide*. To launch the Administration GUI client, use one of the following:

- **Start > Programs > Cisco Prime Network > Prime Network Administration** to launch the full standalone client. You will have to enter the gateway IP address in addition to your credentials.
- **Start > Programs > Cisco Prime Network >** *gateway-ip* **> Prime Network Administration** to launch the Webstart client. You will have to enter your credentials.

Figure 1-1 identifies the basic parts of the Prime Network Administration window.

*Figure 1-1 Prime Network Administration Window*




| | | | |
|---|---|---|---|
| **1** | Menu bar, with main menu choices. | **4** | Content area, the main information and work area of the GUI client. |
| **2** | Toolbar with action icons (what is displayed depends on your selection). | **5** | Shortcut menu, displayed by right-clicking an item in the content area. |
| **3** | Navigation area, which you use to move among the Administration features. | **6** | Status bar, which displays the memory usage of the application process, and connection status. |

### Extending Prime Network and Its Clients

You can download and install new support for NEs, software versions, modules, events, and commands and activation scripts using Prime Network Device Packages (DPs). These can be downloaded from the Prime Network software download site. For more information on how to download and install DPs, see Adding New Device Support with Device Packages, page 4-27.

In addition, advanced users can also extend the features of Prime Network in the following ways.

| To add this extension: | Do the following: |
|---|---|
| Model and display additional NE properties in the Prime Network clients | Use Prime Network Soft Properties to add these properties to the Prime Network clients. Refer to the *Cisco Prime Network 4.2 Customization Guide*. |
| Add support for unsupported devices, software versions, and modules | Use the Prime Network VNE Customization Builder (VCB) to add support for devices, software versions, and modules that are currently unsupported, so they can be displayed in the Vision client. Refer to the *Cisco Prime Network 4.2 Customization Guide*. |
| Add commands and scripts to perform device configurations | Use Prime Network Command Manager to create scripts and commands that users can launch from an NE's right-click menu in the Vision client. These can range from simple show commands to command scripts containing wizards with multiple pages and input methods, such as check boxes and drop-down lists. Refer to the *Cisco Prime Network 4.2 Customization Guide*. |
| Create configuration and activation workflows | Use Prime Network Transaction Manager to schedule and run transactions (workflows) that are created using the Prime Network XDE Eclipse SDK. Refer to the *Cisco Prime Network 4.2 Customization Guide*. |
| Add support for new events | Use the Prime Network VNE Customization Builder (VCB) to add support for traps and syslogs that are currently unsupported so they can be managed by Prime Network. You can also use the VCB to customize the behavior of supported events. Refer to the *Cisco Prime Network 4.2 Customization Guide*. |
| Add new threshold-crossing alarms | Use Prime Network Soft Properties to create TCAs that are generated when a condition you specify occurs. These TCAs can be viewed in the Prime Network clients. Refer to the *Cisco Prime Network 4.2 Customization Guide*. |
| Add external launch points to the Vision client | Add a launch point to an external application or URL to an NE's right-click menu using the Prime Network Broadband Query Language (BQL). Launch points can be added to network elements, links, tickets, and events. Refer to the *Cisco Prime Network 4.2 Customization Guide*. |
| Integrate with northbound applications | Integrate with northbound APIs using BQL to extend the Prime Network Information Model Objects (IMOs), which provide a generic information representation. Refer to the *Cisco Prime Network Integration Developer Guide*. |
| Support Multi-Technology Operations Systems Interface (MTOSI) and 3GPP northbound interfaces (licensed separately) | Install a Prime Network integration layer that allows Prime Network to expose MTOSI and 3GPP APIs over Service Oriented Access Protocol (SOAP). You can also schedule regular 3GPP inventory reports (by choosing **Tools > Web Service Scheduler** from the Administration client or Vision client). Refer to the *Cisco Prime Network OSS Integration Guide for MTOSI and 3GPP*. |
| Integrate Cisco Multicast Manager (CMM) with Prime Network | Add CMM launch points to the Administration and Vision client Tools menus. Follow the instructions in the *Cisco Prime Network 4.2 Installation Guide*. |

# Setting Up Redundancy, Data Purging, and Other Stability Settings

### Create Unit Protection Groups and Designate Standby Units

When you install Prime Network on a unit, the installation procedure queries whether the unit will be a standby unit. A standby unit comes online when a unit in its protection group fails. By default, all units are added to a protection group called default-pg. You can get information on unit and process protection from Overview of Unit and Process Protection, page 5-1.

**Note** Gateway high availability is described in the *Cisco Prime Network 4.2 Gateway High Availability Guide*.

### Adjust Data Purging

To protect system stability and performance, Prime Network purges data from the system at regular intervals, depending on the data type. While the default settings are normally sufficient, you can adjust them if necessary as described in Controlling How Data is Saved, Archived, and Purged, page 8-3. The following table lists the default settings for data purging.

**Caution** Consult with your Cisco account representative before changing these settings. Making the settings smaller could result in immediate and permanent removal of fault data. Making the settings larger could result in slow data retrieval performance; the system might require additional storage and some database tuning; and backups might require more time.

For information on Operations Reports and the Infobright database, refer to the *Cisco Prime Network 4.2 Operations Reports User Guide*.

| Data | Purged After (Default): | To change the setting, see: |
|---|---|---|
| Tickets and events in Oracle database | 14 days after events are archived | Adjusting the Fault Database Purging Settings, page 8-11 |
| Jobs | Never purged | Purging Jobs, page 8-12 |
| Reports—Prime Network standard reports | 90 days | Purging Reports, page 8-12 |
| Backups of gateway data for systems with external Oracle database | 5 backups | Changing these settings is not recommended. |
| Backups of gateway data for systems with embedded Oracle database | 16 backups | |
| Backups of database for systems with embedded Oracle database | 8 days | |
| Monitoring (Graphs) tool | 29 days | Cannot be changed. |
| Configuration Archive files and change logs | 30 days | *Cisco Prime Network 4.2 User Guide* |
| Software Images | n/a (manual deletions only) | Cannot be changed. |

### Control the Maximum Number of Client Sessions for a Gateway

By default, a maximum of 150 clients can be connected to the gateway at one time. This is a system-wide setting. You can adjust this setting, but you should not make it higher than 150 (otherwise system performance may be negatively impacted).

User accounts also have a connection limit. This is a per-user setting. A user will not be able to log in if the system-level setting has been reached, or their per-user limitation has been reached.

To adjust the system-wide setting, see Managing Client and User Sessions, page 3-20. To control the per-user setting, see Creating a New User Account and Viewing User Properties, page 7-9.

**Note** Prime Network users can view reports only if an additional user session is configured in their Prime Central user management settings. This is because Prime Central gives Prime Network users one session by default, but the reports function requires an additional session. Refer to the *Cisco Prime Central User Guide* for more information.

### Specify When Events Are Removed from a Vision Client Inventory Window

When an inventory window is opened from the Vision GUI client, it displays an Inventory Event Viewer (normally at the bottom of the window) that lists the recent events for that device. By default, only events that occurred in the last 6 hours are listed. To change this setting, see Controlling the Vision Client Event Displays (Standard Events, History Size), page 9-24.

# Setting Up the Regular Backup Schedule

Prime Network deployments can include an embedded or external Oracle database. The following topics describe the default backup settings for data stored in the Oracle embedded database or on the gateway.

**Note** For information on setting up a backup schedule for the Infobright database (used by Operations Reports), refer to the *Cisco Prime Network 4.2 Operations Reports User Guide*.

An Oracle database can be embedded or external:

- Systems with an embedded Oracle database—Prime Network enables the backup mechanism during installation and backs up both the database and gateway data. If you did not enable the backup mechanism, use the procedure in Enabling Embedded Oracle Database Backups, page 2-11. An embedded database backup also backs up data that is stored on the gateway. The schedule for the backup depends on your database profile.
- Systems with an external Oracle database—Prime Network only backs up the gateway data; it does not back up the external Oracle database. You must back up external Oracle databases yourself.

**Note** You should save backups to tape on a daily basis.

The following table shows the default backup schedule for systems with embedded and external Oracle databases. (*Actionable events* are events that are of interest to Prime Network. For more details about actionable events, see How Prime Network Handles Incoming Events, page 9-1).

| System with: | Default Backup Schedule |
|---|---|
| Systems with embedded Oracle database | Database information is backed up according to the database profile entered at installation:<br>• 1-20 actionable events per second—Full backup is performed Saturday at 1:00 a.m.; incremental backups are performed Sunday-Friday at 1:00 a.m.<br>• 21-250 actionable events per second—Full backup is performed Tuesday and Saturday at 1:00 a.m.<br>Gateway data is also backed up. |
| Systems with external Oracle Database | Gateway data is backed up every 12 hours at 4:00 a.m. and 4:00 p.m, as defined in the crontab file.<br>**Note** The external Oracle database is not backed up by Prime Network. Follow your vendor documentation to back up your external Oracle database. |

For complete information on the backup and restore mechanism and its configurable points, see Backing Up and Restoring Data, page 2-5.

# Setting Up Fault Monitoring

### Setting Up Prime Network to Receive Events from Devices and Process Them

Make sure that Prime Network is properly configured to receive and save events. You may want to refer to How Prime Network Handles Incoming Events, page 9-1, which provides an illustration of how events are handled by Prime Network.

Check the configuration of the Event Collector, AVM 100. During installation, Prime Network creates Event Collectors on the gateway and all units, but *only* the gateway Event Collector is started. As VNEs are added, they will automatically register with that Event Collector. Check Setting Up the Event Collector: Supported Scenarios, page 9-7, to make sure you are using the configuration appropriate to your deployment.

Check the configuration of the Fault Agent, AVM 25. The Fault Agent runs on all units and creates tickets based on correlation and event type information, and sends information to the Oracle Fault Database so it can be saved and viewed in the GUI clients. AVM 25 *always* requires Oracle database connectivity. If a connection is not available, you can configure AVM 25 to use a proxy AVM 25. (See Configuring a Proxy Database Connection for Units Not Connected to Database, page 9-16.)

### Configuring Devices to Forward Events to Prime Network

All devices you want Prime Network to manage must configure devices to forward events to Prime Network (where the Event Collector, AVM 100, is running). If you want Prime Network to forward events from unmanaged devices, you must enable notification from unmanaged devices using the procedure in the *Cisco Prime Network Integration Developer Guide*.

Before you add devices to Prime Network (by creating VNEs), be sure to provide all necessary device configuration tasks so that when the VNE is created, Prime Network can properly connect to the device, discover it, and monitor it. Prime Network will automatically choose the best *VNE scheme* according to device type. A VNE's scheme determines what data will be retrieved for each device, and which commands and protocols Prime Network should use to collect that data. You can also configure a new scheme that will model and monitor the specific information you want.

For information on device configuration tasks, see Configuring Devices So They Can Be Properly Modeled and Managed by Prime Network, page A-1. For information on supported schemes and technologies, seethe *Cisco Prime Network 4.2 Supported Technologies and Topologies*.

### Creating E-mail Notifications for Important Events and Tickets

You can configure Prime Network to generate e-mail notifications when an event or ticket occurs. You can base it on severity, type, and other criteria. For information on how to create an Event Notification Service, see Configuring Trap and E-Mail Notifications (Event Notification Service), page 9-17.

### Forwarding Event and Ticket Information to Other Applications

You can also use the Event Notification Service to forward specific events and event information to other NMSs or as an e-mail notification. This is described in Configuring Trap and E-Mail Notifications (Event Notification Service), page 9-17.

### Disable Ticket Management from Prime Network Vision and Prime Network Events

If you do not want Vision and Events clients users to manage tickets, you can disable this function. This is helpful when you only want to manage tickets through BQL or the external OSS. To disable the ticket actions, see Disabling Ticket Management in the Prime Network Vision and Events Clients, page 9-23.

# Setting Up Change and Configuration Management

Change and Configuration Management manages the software images and device configuration files for devices in your network. There are a number of tasks you should perform to ensure that Prime Network can properly perform these operations.

- Make sure your devices are properly configured as described in Configuring Devices So They Can Be Properly Modeled and Managed by Prime Network, page A-1.
- From the Administration client, specify when a software image distribution operations should time out. The default is 30 minutes. To change the setting, choose **Tools > Registry Controller > Image Management Settings > Image Distribution**, adjust the timeout, and click **OK**.
- From the Administration client, specify if you require the distribution server. To add the distribution server, choose **Tools > Registry Controller > Image Management Settings > Image Distribution**, select **True**, and click **Apply**.
- From the Vision client, follow the tasks that are documented in the *Cisco Prime Network 4.2User Guide* (where CCM setup is addressed).

# Setting Default Credentials for VNEs

When you create default settings for the SNMP and Telnet/SSH protocols, the settings are automatically applied to all new VNEs.

To configure default VNE settings, choose **Global Settings > Default VNE Settings**.

- **Telnet SSH Setting** are described in Telnet/SSH VNE Properties Reference, page D-6.
- **SNMP Settings** are described in SNMP VNE Properties Reference, page D-5.

To find out what version of SNMP or SSH a VNE is using, right-click the VNE and choose Inventory. This opens the device inventory window, click **VNE Status**. See Figure 4-11 on page 4-47 for an example.

# Changing the Minimum Role Required for the Administration and Events Clients

By default, only users with Administrator privileges can log into the Administration client and the Events client. If you want to adjust these roles, do the following:

- Use the Registry Controller to change the role required to use the Events client.
- Use the registry editor command line interface to change the role required to use the Administration client.

Both procedures are described in Changing the Minimum User Access Role for the Events and Administration Clients, page 7-13.

# Setting Up External User Authentication

**Note** If you are using Prime Network with Cisco Prime Central, external authentication is disabled. See Using Prime Network with Cisco Prime Central, page 1-12.

If you want to use external authentication, you must configure Prime Network to communicate with the LDAP server. See Configuring Prime Network to Communicate with the External LDAP Server, page 7-18. If you are switching from external authentication to Prime Network authentication, you can import the user information from the LDAP server into Prime Network. That procedure is described in the Importing Users from the LDAP Server to Prime Network, page 7-21.

# Creating User Accounts and Device Scopes for Authentication and Authorization

**Note** If you are using Prime Network with Cisco Prime Central, the following features are disabled. See Using Prime Network with Cisco Prime Central, page 1-12.

### Adjusting Global Rules for User Passwords

By default, Prime Network uses the following password rules

| Password Rule | Default |
|---|---|
| Password validity period | 30 days |
| When to begin sending reminders of pending password change | 7 days before validity period ends |
| Permitted attempts before lockout | 3 attempts |

| Password Rule | Default |
|---|---|
| Password must be different from ___ previous passwords | 5 passwords |
| Password must contain at least four different character types | Enabled |
| Password cannot contain any character that is repeated more than twice consecutively | Enabled |
| Password cannot contain ___ consecutive characters from the previous password | 4 characters |
| Password cannot contain a replication or reversal of the user name | Enabled |
| Password cannot contain the word _____ | Cisco |

#### Adjusting the Timer for Disabling Accounts Due to User Inactivity

By default, if a user does not log into their account for 30 days, their account is disabled. A disabled account must be re-enabled by a user with Administrator privileges. You can adjust this period if necessary. See Configuring Global User Permissions: Account Inactivity, Device Credential Requirements, and Global Job Scheduling, page 7-6.

#### Requesting User Credentials Before Running Command Scripts and Transactions

You can configure Prime Network to require users to enter their credentials when they execute command scripts from these features:

- A device's right-click **Commands** menu in the Vision GUI client (applies only to commands that are immediately executed; does not apply to scheduled commands)
- Transaction Manager
- Change and Configuration Management (includes Compliance Audit)

The user name is also added to Provisioning and Audit events.

This mode is disabled by default. See Configuring Global User Permissions: Account Inactivity, Device Credential Requirements, and Global Job Scheduling, page 7-6.

#### Displaying a Warning Message When Users Run Command Scripts

You can configure Prime Network to display a warning message whenever users execute command scripts from these features:

- A device's right-click **Commands** menu in the Vision GUI client (applies to commands that are executed immediately and commands that are scheduled)
- Command Manager repository

Users must acknowledge the message before proceeding. By default, no message is displayed. See Adding a Warning Message to Command Scripts, page 10-2.

#### Controlling Who Can Execute Jobs in Prime Network Features

Prime Network provides a global per-user authorization mechanism that controls whether a user can execute an action that uses the Job Manager. This includes jobs launched from:

- A device's right-click **Commands** menu in the Vision GUI client (applies to scheduled commands only; commands that are executed immediately do not use the Job Manager)
- Change and Configuration Management (CCM), Compliance Manager, Command Manager, Transaction Manager

Enabling and disabling this mode is controlled from global security settings. If the mode is enabled, job scheduling privileges are controlled by a setting in the individual user accounts.

- If this mode is enable and a user is granted privileges, the user can schedule jobs across the product.
- If this mode is enabled and a user is not granted privileges, the job scheduling features in the user's GUI clients are disabled.

If the global per-user authorization mode is disabled, all users can schedule jobs; the setting in the users's account is ignored.

By default, in Prime Central, this mode is disabled which means job scheduling privileges are controlled by the settings in individual user accounts. See Configuring Global User Permissions: Account Inactivity, Device Credential Requirements, and Global Job Scheduling, page 7-6.

#### Allowing Shared (Public) Reports

Prime Network also provides a global authorization mode for creating shared or public reports.When a report is public, all users can view the contents; reports are *not* filtered according to scopes or security privileges. Enabling and disabling this mode is controlled from global security settings. If the mode is enabled, all users can create shared reports.

This mode is disabled by default, which means no users can create public reports. Configuring Global Report Security Settings (Public Reports), page 7-8.

#### Creating Accounts So Users Can Log Into Prime Network

Only a *root* user account created when you install Prime Network. The root user can then create accounts for other users. The settings in individual user accounts specify the GUI tasks the user can perform.

In addition, the devices a user can see and manage is determined by the device scopes that are assigned to their user account. Device scopes are groups of devices that can be configured and named according to your deployment needs. When you assign a device scope to a user's account, you also choose a security level for that scope. As the user role determines the GUI tasks a user can perform, the security level determines the tasks a user can perform on devices in the scope. Only one device scope is created by default, the All Managed Elements device scope.

For information on creating user accounts and device scopes, see User Authentication and Authorization Overview, page 7-2.

# Creating Login Banners

You can create a message of the day or banner, which is displayed whenever a user logs into a GUI client or the gateway server. See Creating a GUI Client Banner Message, page 11-13.

You can also create a message that is displayed when users execute certain command scripts. See Adding a Warning Message to Command Scripts, page 10-2.

# Setting Up Regular Reports

Prime Network provides Operations Reports feature for generating the data you need to manage your network, devices, and the Prime Network system. The Operations Reports feature provides prepackaged reports for information on data center (VMs) and mobility deployments (access points), along with fault and inventory reports. In addition, you can use the drag-and-drop interface to create customized interactive reports. For information on how to use Operation Reports, refer to the *Cisco Prime Network 4.2 Operations Reports User Guide*.

# Using Prime Network with Cisco Prime Central

Prime Network can be installed as a standalone product or with Cisco Prime Central. When installed with Prime Central, you can launch Prime Network GUI clients from the Cisco Prime Portal:

- Launch Prime Network Administration from the **Administration** tab by selecting **Discovery/Adding Devices > Prime Network** or **Scope Management > Prime Network**.
- Launch Prime Network Vision and Events from the **Assure** tab.

The Cisco Prime Portal uses a single sign-on (SSO) mechanism so that users need not re-authenticate with each GUI client. All session management features are controlled by the portal (such as client timeouts). If a user tries to log into a standalone GUI client, the user will be redirected to the portal login. The only exception is the emergency user, who will still be allowed to log into a standalone GUI client.

When Prime Network is in suite mode:

- Most of the choices in the Global Settings > Security Settings branch are disabled. This includes configuring user accounts, the user authentication method, password rules, and so forth.
- You can still control whether users will have to enter their credentials whenever they perform device configuration operations, and whether all users have job privileges. By default these are both enabled. To change those settings, see Configuring Global Report Security Settings (Public Reports), page 7-8.
- Ticket operations from Prime Network remain enabled. You can disable them by following the procedure in Disabling Ticket Management in the Prime Network Vision and Events Clients, page 9-23.

Prime Network sends the suite regular information about Prime Network server health (ping, CPU usage, and memory usage). At hourly intervals, Prime Network checks the suite for any changes that should be reflected in Prime Network.

Cross-launch to and from other suite applications is also supported. The applications share a common inventory. The *Cisco Prime Network 4.2User Guide* describes how to set up and use Prime Central. Keep these operational items in mind when using Prime Network with Prime Central:

- When you create new VNEs, use the device SYSNAME as the VNE name. This allows other suite applications to recognize the device. Also, do not use **None** or **All** as the SYSNAME, because those names have internal meaning to Cisco Prime Central.
- If you migrate from standalone to suite mode, all user security roles are migrated to the suite, but device scopes are not migrated. After the migration is complete, you must create user accounts in Prime Central, using the same username that were used in standalone Prime Network. Prime Central will advise you that the user already existed in Prime Network and will retrieve the user properties and apply them to the new Prime Central user.

  Prime Network users will only be allowed to view reports if an additional session is configured in their Prime Central user management settings. This is because Prime Central gives Prime Network users one session by default, but the reports function requires an additional session.
- If the Cisco Prime Performance Manager application is also installed, the Prime Network Event Collector will receive threshold crossing alarm (TCA) events from Prime Performance Manager components and do the following:
  - Save TCA events in the Oracle Fault Database.
  - Forward TCA events to appropriate VNEs.

  No special configuration is required but check the *Cisco Prime Network 4.2 Release Notes* to make sure the versions of Prime Network and Prime Performance Manager are compatible.

Prime Network also receives EPM-MIB traps from the network. By default Prime Network receives EPM-MIB traps from any source in the network. If desired, you can configure Prime Network to only process EPM-MIB traps arriving from a specific Prime Performance Manager server. The instructions for doing this are provided on the Cisco Developer Network at https://developer.cisco.com/site/prime-network/.