Next Steps

This chapter provides some steps you should perform after installing the product. After you perform these steps, you can move on to use the Prime Network Administration GUI to add users, create device scopes, and so forth.

Launching the Prime Network GUI Clients

Prime Network enables you to access all its GUI clients from the Web Start page on the gateway. It provides single sign on for all GUI clients. After you enter your credentials, you can access any of the clients.

Before You Begin

Verify the following:

- All the client requirements are met. For more information on the requirements, see Prime Network Client Requirements, page 2-11.
- Java 8 update 60 is installed on your computer. If not, download it from the Java download site: *http://www.java.com*.

  Note Prime Network was tested on Java 8 update 60, however it is expected to work with lower Java 8 updates as well.

- Ports 6080 and 6081 are open. For other ports required for Prime Network, see Required Ports for Prime Network, page 2-24.

To access the clients using Java Web Start technology:

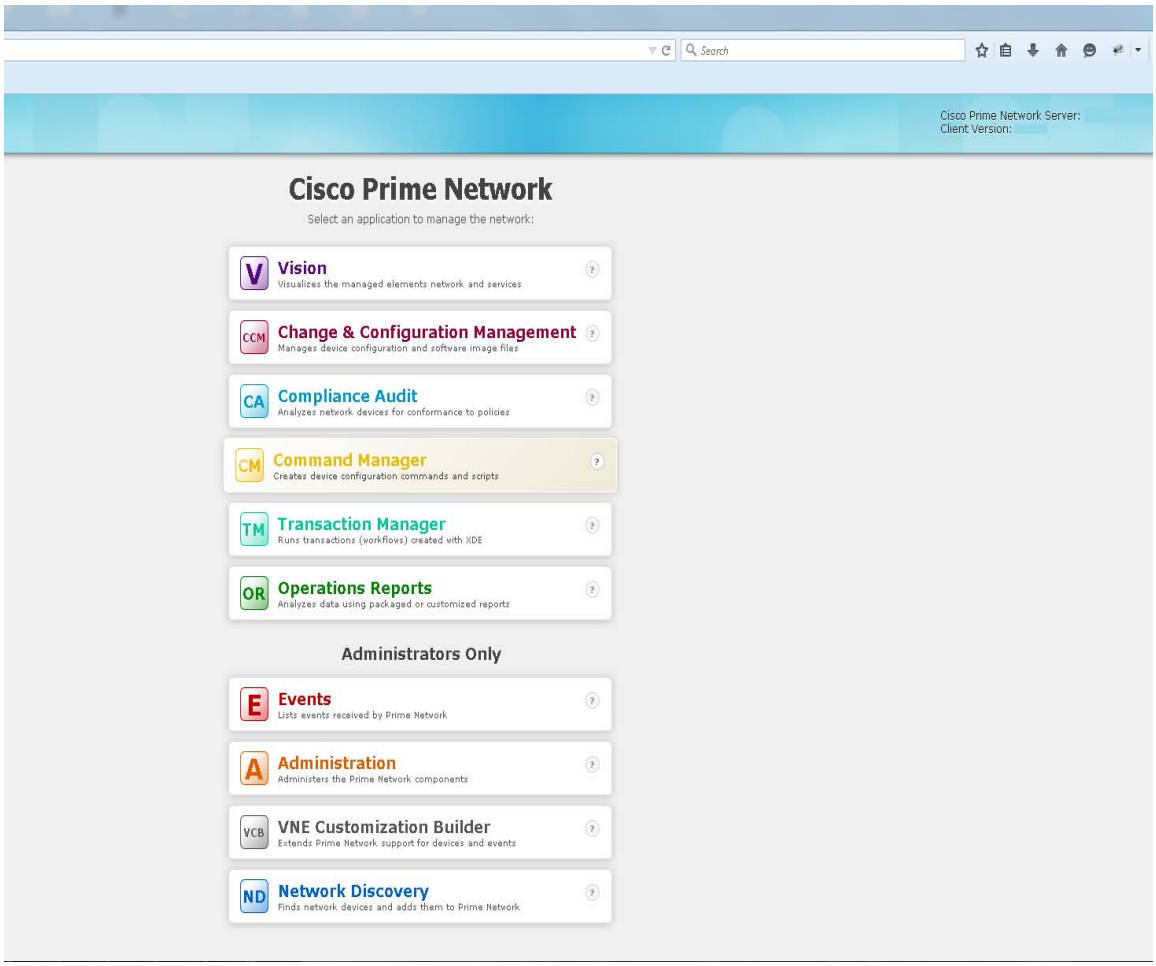
Step 1 Log into the gateway by entering:

`http://`*`gateway-host-ip`***`:6080/ana/services/install/install/webstart.html`**

where *gateway-host-IP* is the gateway host name or IP address.

Step 2 Enter your user name and password in the Prime Network login window and click **Login**.

The Prime Network applications launch page is displayed and provides access to all of the Prime Network GUI clients.



Step 3 Click on the Prime Network application you want to access. A.jnlp file is downloaded.

Step 4 Click **Continue** in the Security Warning screens. The client application jar files are downloaded and the Prime Network application starts.

Verifying That Backups Are Set Up

The Prime Network backup and restore process includes:

- Data backup of the registry data, encryption keys, and reports using the operating system cron mechanism. This data is backed up regardless of whether you have an embedded or external database.

- Embedded database backup. For external database, refer to Oracle documentation.

Prime Network performs backups on a regular schedule. The schedule and data that is backed up depends on whether you have a system with an embedded database or an external database.

Note Back up to tape on a daily basis.

Verifying the Prime Network Data Backup (Gateway Data)

To verify that Prime Network is backing up your data, check the backup directory after you expected a backup to occur. By default the data is saved in $*NETWORKHOME*/backup. For information on changing the backup schedule or location, or performing a manual backup, see the Cisco Prime Network 4.2.3 Administrator Guide.

Verifying the Embedded Database Backup

Embedded database backups are normally enabled during installation. If you did not enable them, use the procedure in *Cisco Prime Network 4.3.2 Administrator Guide.* You must enable this mechanism if you want to perform a backup of the embedded database, regardless of whether the backup is manual or automatic.

Embedded database is backed up according to the profile selected at installation:

- **1-50 actionable events per second** —Full backup is performed every Saturday at 1:00 a.m.; and incremental backups are performed every Sunday-Friday at 1:00 a.m.
- **51-250 actionable events per second** —Full backup is performed every Tuesday and Saturday at 1:00 a.m.

To verify that backups are happening, after a sufficient amount of time has lapsed, check the backup directory you specified during installation.

Operations Reports Data Backup

For information on performing a reports data backup, see the *Cisco Prime Network 4.3.2 Administrator Guide.*

Enabling Network Discovery

If you did not configure Prime Network during the initial installation process, you must enable the network discovery functionality manually, as follows:

Step 1 As the root user, navigate to the Prime Network home directory/local/scripts/. Be sure to enter the full path to the home directory.

Step 2 Execute **setFpingPermissions.tcsh**.

Example:

```
/export/hone/pn431/local/scripts/setFpingPermissions.tcsh
```

Setting Up Transaction Manager

Transaction Manager replaces the Prime Network Workflow and Activation functionality that was available in previous releases of Prime Network. Transactions are activation workflows that you can create using the XDE Eclipse SDK, and then execute from Transaction Manager.

For information on the Transaction Manager GUI and how to use it, see the *Cisco Prime Network 4.3.1 Customization Guide*.

To install the XDE Eclipse SDK, contact Advanced Services.

Setting Up VMware vCenter to Forward Events

Prime Network uses the VMware vCenter to obtain information about virtualization inventory and events information by modeling the vCenter as an individual VNE. The XMP Datacenter component retrieves events from the VMware vCenter, normalizes them into the CISCO-EPM-NOTIFICATION-MIB trap format, and forwards them to the Event Collector (AVM 100).

To receive events from the VMware vCenter, you must perform one of the following procedures so that the XMP Datacenter will send UCS events to the correct Event Collector location.

If the Event Collector (AVM 100) is running on:	You must do the following (as Linux root user):
A different server from XMP_DATACENTER	1. Go to $*NETWORKHOME*/Main/XMP_DATACENTER/conf. 2. In the datacenterevent.properties file, set the value of the following property to the IP address of the server running AVM 100: **datacenterevent.destAddress0**
The same server as XMP_DATACENTER	**iptables -t nat -A OUTPUT -p udp -d localhost --dport 162 -j REDIRECT --to-port 1162**

Integration with Cisco Multicast Manager (CMM)

Prime Network provides multicast support by enabling integration with Cisco Multicast Manager 3.3.2 (CMM). This involves installing CMM on the Prime Network gateway server, and then manually creating the menu options that will enable cross-launching CMM from the Prime Network Administration and Vision GUI clients.

Note In an installation scenario, where the Cisco Prime Network is installed first followed by the Cisco Prime Network Operations Reports and the CMM on a gateway server, the application might shutdown. In such case, restart the CMM application and then enter the following system command as a root user: **service mysqld-ib start**.

Setting Up Integration with Cisco Multicast Manager

To integrate Prime Network with CMM:

Step 1 Install CMM on the Prime Network gateway server. Refer to the *Installation Guide for Cisco Multicast Manager*.

Step 2 Log into the gateway as *pnuser*.

Step 3 Change directories to $*NETWORKHOME*/Main/ and enter the following command:

```
installCMMLaunchMenu.pl
```

Step 4 At the prompt, enter the port to be used by CMM (default 8080 but this might have been changed during CMM installation).

Step 5 When the registry files have been updated, you will be notified that the CMM launch menu has been added successfully.

Step 6 Restart the Prime Network Administration and Vision GUI clients.

Step 7 In Prime Network Administration, verify that the CMM Configuration menu option appears in the Tools menu. In Prime Network Vision, verify that the CMM Dashboard menu option appears in the Tools menu.

Setting Up Traps for CMM

To receive CMM traps in the **Trap Viewer** page:

Step 1 View the status of IP tables, and verify if the 2162 port is configured by entering the following command:

#iptables -t nat -L -n -v

Step 2 Change the rules in IP tables in the **/usr/sbin** directory by enter the following CLI command:

```
#iptables -t nat -A PREROUTING -p UDP --dport 162 -j REDIRECT --to-port 2162
```

Step 3 In the snmptrapd.conf file, under **/usr/local/netman/mmtsys/share/snmp** directory, enter the following command in the first line and save.

```
snmpTrapdAddr udp:<server-ip>:<port-no>
```

For example, **snmpTrapdAddr udp:10.106.214.116:2162**

Note Ensure that the port number is provided as 2162.

Step 4 Restart CMM by entering the following commands:

```
#/usr/local/netman/K98mmt
#/usr/local/netman/S98mmt
```

Step 5 Launch the CMM GUI and verify if the CMM traps are received in the **Trap Viewer** page.

Removing Cisco Multicast Manager Integration from Prime Network

To remove CMM integration from Prime Network:

Step 1 Log into the gateway as *pnuser*.

Step 2 Change directories to $*NETWORKHOME*/Main/ and enter the following command:

```
uninstallCMMLaunchMenu.pl
```

Step 3 Restart the Prime Network Administration and Vision GUI clients.

Step 4 In Prime Network Administration, verify that the CMM Configuration menu option is removed from the Tools menu. In Prime Network Vision, verify that the CMM Dashboard menu option is removed from the Tools menu.