Manage Control Center

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

This chapter contains the following sections:

Hosts

Hosts allows you to manage the various servers. To access Hosts:

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

The Control Center Hosts window appears.

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

Click any of the buttons and proceed as follows:

- Details, page 2-1—Available only when the host system is chosen.
- Config, page 2-2—Available only when the host system is chosen.
- Servers, page 2-7—Available only when the host system is chosen.
- Watchdog, page 2-7—Available only when the host system is chosen.
- Logs, page 2-8—Available only when no host system selection is made.

Details

For details about a chosen host, follow these steps:

Step 1 Choose a host by checking the check box to the left of the hostname and then click the **Details** button.

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

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

Config

To navigate to the **Properties** pane of the Host Configuration window, perform the following:

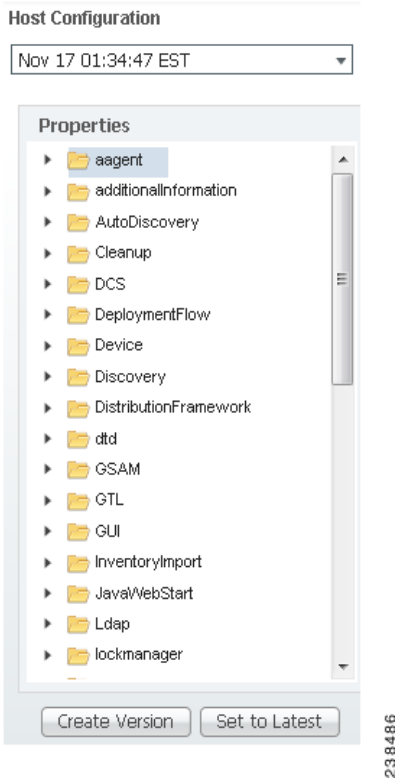
1. In the Control Center Hosts window, check the check box of the hostname.
2. Click **Config**.

You can view or modify Dynamic Component Properties Library (DCPL) properties in the properties pane by following these steps

Step 1 Select a property from the Properties pane as shown in Figure 2-1 to view its explanations, defaults, and ranges/rules.

Note Properties pane contain the details of all the properties in a folder format. If you do not know the property name, you can use a key word and do a Find.

Figure 2-1 Properties



Step 2 Click on the arrow of the property folder.

Note Expand the sub folders till you reach the specific property.

Step 3 Click on the property to view the details and instructions on how to change the value, as shown in Figure 2-2.

Figure 2-2 Properties Detail Example

Step 4 For each property that can be modified, you can modify the value and click **Set Property**. If when making your modifications, you want to return to the previous settings, click **Reset Property**.

Step 5 After making all the changes you choose in each of the specific properties, you can click **Create Version** to create a new version of these properties. This feature gives you the option of saving multiple property sets for future use.

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

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

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

You are able to perform the below mentioned additional tasks using the DCPL properties:

- Supporting Ldap Authentication, page 2-4

Note To perform the below tasks, certificates has to be imported from Prime Network. For more information about this, refer to the section **Integrating with Prime Network for Device Import** in *Cisco Prime Provisioning 7.0 Installation Guide.*

- Configuring Prime Network(s) in Prime Provisioning, page 2-5
- Subscribing or Unsubscribing to Prime Central Device Commission and Decommission Notification, page 2-6

Supporting Ldap Authentication

Prime Provisioning provides support with Ldap authentication for a more secured environment. You can use either **Oracle Directory Service Enterprise Edition 10g and 11g** or **Micrososft Active Directory** as your LDAP server.

To perform authentication using Ldap server, you need to set the following attributes in the DCPL properties section:

- **DistinguishedName**

- **HostName**
- **LdapAuthentication**
- **UserDefinedException**

From Prime Provisioning 6.5.0.5 release, Distinguished Name property supports two formats. If the property contains {0} then it is used as a DN template, otherwise it is used as a DN suffix with uid used as a prefix.

For identifying users within a group or subgroup:

```
Ldap.DistinguishedName=
OU=Employees,OU=Cisco Users,DC=cisco,DC=com
```

This format type is used in **Oracle Ldap.**

Sample result of this format: uid=donaldh,OU=Employees,OU=Cisco Users,DC=cisco,DC=com as the bind DN.

```
Ldap.DistinguishedName=
cn={0},OU=Employees,OU=Cisco Users,DC=cisco,DC=com
```

This format type is used in both Oracle and MS AD Ldap

Sample result of this format: cn=donaldh,OU=Employees,OU=Cisco Users,DC=cisco,DC=com as the bind DN.

In MS AD along with the above format you can mention the DN in two different formats.

For identifying users within a Domain:

```
Ldap.DistinguishedName=cisco\{0}
```

For identifying users from the entire Directory:

```
Ldap.DistinguishedName={0}@<Full Domain Name>
Example: {0}@win.eng.cisco.com
```

For successful authentication, the user must be created in both Prime Provisioning and Ldap server with same or different passwords. But when you login into Prime provisioning by enabling LdapAuthentication, you need to enter the password that was configured in Ldap server.

Configuring Prime Network(s) in Prime Provisioning

In the **Host Configuration** screen, you can configure Prime Network in Prime Provisioning by choosing **Properties > Inventory Import > Prime Network** and modifying the below values:

- **enablePrompts** - Prompts are present on the server so that the Prime Provisioning can execute the web services at the backend.
- **Gateway** - Multiple gateways can be configured by separating the values with a comma. The order in which the Prime Networks are configured has an impact on the inventory import.

```
For example, if there is a device D1 available in two instances of Prime Network
configured in the order PN1 and PN2, inventory import will always import the device from
the first instance PN1 and will ignore the other.
```

- **loginPrompts** - General configuration for the login prompts on the server.
- **logLevel** - Log level for the inventory import log.
- **Password and UserName**
  - Prime Provisioning can interface with Prime Network in both the installation modes: Standalone mode and Suite mode integrated with Prime Central.

- When Multiple Prime Networks are configured either in Standalone or Suite mode, the login credentials provided should be able to access all the instances of Prime Network.

For example, consider a user *admin* is created in Prime Central. In Suite mode, for all the features to work as expected, *admin* should have access to Prime Provisioning with appropriate role and access to Prime Network as **Administrator**. The user should be assigned with the scope of all the Network elements in Prime Network.

In case of Standalone mode, the user should have access to Prime Network as **Administrator** and should be assigned with the scope of all the Network elements in Prime Network. For more information about Prime Network configuration, refer to *Prime Network User Guide*.

- Password provided here is encrypted both at the screen level and also in the database. Be sure to configure a valid value for the Inventory Import, Device Commission and Device Decommission features to function as expected

initdb Script Enhancements to Retain DCPL Values with Configured Values

During Prime Provisioning upgrade, to retain the Dynamic Component Properties Library (DCPL) property values without a reset, use the following CLI commands:

```
./prime.sh stop
./prime.sh startdb
./prime.sh initdb.sh noreset
./prime.sh start
```

The values are retained or updated in the Prime Provisioning repository based on the following criteria.

1. When the *initdb.sh* script is run without any argument, Prime Provisioning reads the DCPL properties from *vpnsc.properties* and updates them in the Prime Provisioning repository.
2. When the *initdb.sh* script is run with *noreset* argument, Prime Provisioning retains the DCPL values which are already configured.

When the *initdb.sh* script is run with some irrelevant argument other than the *noreset* argument, Prime Provisioning will display an error message; “The only supported argument for *initdb.sh* is *norese”*

Subscribing or Unsubscribing to Prime Central Device Commission and Decommission Notification

When Prime Provisioning is either installed in suite mode or upgraded to suite mode, it subscribes to Prime Central device commission and decommission notifications by default. Once subscribed, Prime Central forwards the device commission and decommission notifications received from the other Domain Managers to Prime Provisioning.

To subscribe or unsubscribe to Prime Central device commission and decommission notifications, choose **InventoryImport > PrimeCentral > enableNotification** from the **Properties** pane and proceed as mentioned below**.**

- To receive notifications, set the **property** to **true**.
- To stop receiving notifications, set the **property** to **false**.

To view the notification logs when there is no host selected in the Host window, choose **Logs > PCNotification**. The information related to creation and deletion of a device are captured here.

Servers

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

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

A window as shown in Figure 2-3, appears.

Figure 2-3 Servers

238488

Step 2 Check any one check box next to the server you want to address and you have access to **Start**, **Stop**, **Restart**, and **Logs**. When you click on a specific server name or the Logs button, you get a list of server logs. If you then click on the log name for which you want details, the log viewer appears. You can filter this information in the log viewer. After you complete the task of your choice, you return to Figure 2-3.

Step 3 You can click a different server and click the button for the process of your choice. Or you can unclick the server choice and click **OK**.

Step 4 After you click **OK** in Figure 2-3, you return to the Control Center Hosts window.

Watchdog

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

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

A window as shown in Figure 2-4, "WatchDog Logs," appears.

Figure 2-4 WatchDog Logs

Step 2 Click on a specific WatchDog log name in the **Name** column to get the contents of that log. You can filter the information in this log. Click **OK** to return to Figure 2-4.

Step 3 You can repeat the process in Step 2 or click **OK** to return to the Control Center Hosts window.

Logs

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

Step 1 From the Control Center Hosts window, be sure that no check boxes are checked.

Step 2 Click the **Logs** drop-down list and select **Install** or **Uninstall**.

The window that appears is the log of installations or uninstallations, dependent on your selection in Step 2.

Step 3 Click the link in the **Name** column to view the detailed log information.

Step 4 Click **OK** to return to the window.

Step 5 Click **OK** again to return to the Control Center Hosts window.

Licensing

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

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

To install license keys, follow these steps:

Step 1 Choose **Administration > Control Center > Licensing**, and a window as shown in Figure 2-5, appears.

Figure 2-5 Choose Administration > Control Center > Licensing

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

Note When you purchase a full version license key all features except TE, TE/BRG, TE/RG are activated with unlimited activation and unlimited VPNs.

Note The TE licenses can be purchased separately based on the number of nodes/devices available in the inventory. The total number of devices and corresponding device type, IOS/XR version, and platform info is reported by utilizing the reporting mechanism available with the product. Refer to Reporting Mechanism, page 2-10 for the details of executing a reporting mechanism. When you purchase Traffic Engineering Management (TEM), you automatically receive **TE**, **TE/BRG**, and **TE/RG** licenses. All of these licenses *must* be installed to have access to all the Cisco Prime Provisioning TEM features, including Planning Tools for protection planning (backup tunnels). The **TE** license serves as an activation license for the maximum number of TE-enabled nodes to be managed by TEM (you purchase licenses and upgrade licenses based on a range of nodes); the **TE/RG** license enables primary tunnel placement; and the **TE/BRG** license enables the Fast ReRoute (FRR) protection function

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

Step 4 Click **Save**.

Your newly installed license appears in an updated version of the Installed License table, as shown in Figure 2-5.

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

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

Reporting Mechanism

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

To execute the reporting tool, follow these steps:

Step 1 Source the environment from provisioning home directory.

./prime.sh shell

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

```
$PRIMEF_HOME/resources/nbi/scripts/getDevices
$PRIMEF_HOME/resources/nbi/scripts/queries/DevicesQuery
$PRIMEF_HOME/resources/nbi/scripts/util/Login
$PRIMEF_HOME/resources/nbi/scripts/util/checkForErrors
```

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

./getDevices

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