Next Steps

The following topics section describes the next steps you might perform to get started with Cisco Prime Provisioning. Procedures are intended to get you up and running quickly. For more information and details, see the *Cisco Prime Provisioning 7.2 User Guide*. Use the information described in this chapter in the following order:

Restoring Your Sybase Repository to a New Server

If you are restoring your Sybase repository from your original server to a new server, you must first do the following:

Step 1 Run the Prime Provisioning command **./prime.sh stop**

Step 2 **cd /var/tmp** and remove (or save, if needed) all the files under these directories.

Step 3 Back up the **$PRIMEF_HOME/Repository** on the new server, using the command: **mv Repository Repository.bkp**

Step 4 Run the Prime Provisioning command **./prime.sh stop**.

Step 5 **cd $PRIMEF_HOME/Repository**

Step 6 Copy the Repository directory from the original server onto the Prime Provisioning repository on the new server. You can tar up the full Repository directory and untar in the same location on the new server.

Step 7 On the new server, run the Prime Provisioning command **./prime.sh startdb as the Prime Provisioning installation owner.**

Step 8 Run the Prime Provisioning command **./prime.sh initdb.sh as the Prime Provisioning installation owner.**

Step 9 Run the Prime Provisioning command **./prime.sh startwd as the Prime Provisioning installation owner.**

Configuring HTTPS

To configure the secure web access to Prime Provisioning, set up the Hypertext Transfer Protocol (HTTP) Over Secure Socket Layer (SSL) (HTTPS) port, as follows:

Note If you configure HTTPS, it does not disable HTTP. If you want to only allow HTTPS, then you need to block HTTP (default port: 8030) by a firewall.

Step 1 Run the command: **configSecurePort.sh** <*PRIMEF_home*> <*https_port*> <*hostname*>

where:

<*PRIMEF_home*> is the home directory for Prime Provisioning, for example: **/opt/PrimeProvisioning**

<*https_port*> is the secure HTTPS port you want to use, for example: **8443**.

<*hostname*> is the name of the machine that Prime Provisioning is installed on, for example: **machinename.cisco.com**

Step 2 If this is the first time you are logging into Prime Provisioning, you will need to accept the self-signed, untrusted security certificates.

Step 3 If you are using Internet Explorer, accepting the security certificates is not sufficient. You need to place them in the Trusted Certificate store to ensure that the security notifications do not pop up during every login.

Step 4 To place certificates in the Trusted Certificate store:

a. Enter the Prime Provisioning URL in your browser. A security warning is displayed with the message "There is a problem with this website's security certificate, choose Continue to this website (not recommended)."

b. Click **Continue**. This redirects you to the Prime Provisioning Login page

c. Click **Certificate Error** displayed next to the address bar.

d. Click **View certificates**.

e. Click **Install Certificate**.

Note If Installed certificates are not visible, Internet Explorer should be run as an administrator.

f. Click **Next** in the Certificate Import Wizard.

g. Select **Place all certificates in the following store**.

h. Click **Browse** and then click **Trusted Root Certification Authorities**, and click **OK**.

i. Click **Next** in this wizard until you reach the last screen.

j. Click **Finish**.

k. If you get another Security Warning message box, click **Yes**.

l. Click **OK**.

Note If you specify an IP address instead of a hostname, you must then use this IP address for all HTTPS sessions. If you attempt to use the hostname after configuring with an IP address, you will receive hostname mismatch warnings and might see unexpected behavior while using Prime Provisioning.

Logging In for the First Time

To log into Prime Provisioning for the first time, follow these steps:

Step 1 In the browser, enter the following URL:

`http://`*`server:port`***`/isc/`**

Note If you are using HTTP, the default for *server:port* is <*HOSTNAME*>**:8030**.

If you are using secure HTTPS access, as explained in the "Configuring HTTPS" section on page 5-2, enter **`https://`***`server:port`***`/isc/`** instead. The default for *server:port* in this case is <*HOSTNAME*>**:8443**.

In both of the above cases: <*HOSTNAME*> is the UNIX workstation name (or IP address) of the server to which you installed Prime Provisioning.

See Installing Prime Provisioning, page 3-2 for information about the installation log.

Step 2 Enter the default administrative login name, **admin**, and password, **cisco**, then click **Login**.

This default user provides administrative access to Prime Provisioning. You cannot delete this user.

Step 3 We highly recommend you change the password for **admin** from **cisco** to something secure for you. To do this, click the **Administration** tab, then click **Security**, then click **Users**. Check the **admin** check box and then click **Edit**.

The window appears which allows you to change the password and other details.

Step 4 Enter the **Security** and **Personal Information**, then click **Save**.

Installing License Keys

To obtain your license keys please contact: isc-licensing@cisco.com.
To install license keys, do the following:

Note For detailed instructions, see the Licensing section in the *Cisco Prime Provisioning 7.2 User Guide*.

Step 1 From the **Home** page of the installed Prime Provisioning product, navigate as follows: **Administration > Control Center > Licensing**.

Step 2 From the **Installed Licenses** table, click **Install**.

Step 3 In the resulting 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 Licenses table.

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

Note Clear the cache in your browsers to display menus (for example Traffic Engineering or Diagnostics) that might not be displayed after installing license keys.

Importing Device(s) from Prime Network

You will be able to import device(s) from Prime Network to Prime Provisioning using Inventory Manager. When Prime Provisioning is installed in Suite mode, certificate(s) needs to be imported from Prime Network to Prime Provisioning keystore for this feature to work as expected.

A script is available for configuring Prime Network properties and for importing the certificates from Prime Network and this script needs to be executed from the server where Prime Provisioning is installed. You are also able to update the Prime Network properties using DCPL properties. For more information about configuring Prime Network properties using DCPL, refer to *Cisco Prime Provisioning 7.2 Administration Guide*.

When a device is found in multiple instances of Prime Network, Prime Provisioning always imports the device from the first instance of the Prime Network. Connecting to the multiple instances of Prime Network and importing certificates from them is also handled within the script.

Prerequisites

To execute the script successfully, you need to know the following details:

- Prime Network Gateway details
- UserName, Password and Installation path of the server where the Prime Network is installed

```
For example, if Prime Network is installed on SERVER1, then provide the details of this
server as the input for the script when prompted.
```

To import certificates from Prime Network to the Prime Provisioning trust store:

Step 1 Log into Prime Provisioning server.

Step 2 Run the following configuration script in the directory `<PRIMEF_HOME>/bin`.

Tip PRIMEF_HOME refers to the directory where Prime Provisioning is installed.

- configurePN.sh [-a]
  - To set/reset Prime Network application username and password.

Prime Provisioning assumes that the application credentials provided here are the same across all the Prime Network instances. The user has the appropriate scope defined in Prime Central and is also assigned with the "Administrator" role on Prime Network.

Please refer to Prime Central and Prime Network documentation for further information.

Note User can alternatively use the DCPL Properties from GUI to update these details.

- To configure additional Prime Network Gateways.

  Prime Provisioning considers the order in which the gateways are configured, consider if PN1 is configured first, followed by PN2. Prime Provisioning first queries PN1 to import the devices and if the device is found in PN1, it will not interface with PN2. Prime Provisioning interfaces with PN2 only in case if the device is not found in PN1.

Note User can alternatively use the DCPL Properties from GUI to update the gateway details as comma separated values.

- To copy and import the certificates from the configured Prime Network instances.

- configurePN.sh [-c]

  To copy and import the certificates for the existing Prime Network Gateway(s). You are prompted to provide the user name, password, and home directory of the server on which Prime Network is installed. For example, the server credentials can be of the format, **pnuser** for the username, **test** for password, and **/export/home/primenetwork** for the directory where Prime Network is installed.

- configurePN.sh [-d]

  When the user tries to delete a configured Prime Network gateway using this option, it deletes the certificate and also updates the gateway details. After deletion, you need to stop and restart Prime Provisioning server using **./prime.sh stop** and **./prime.sh start** commands.

Tip Deleting a gateway from the DCPL properties does not remove the certificate from the Prime Provisioning trust store. So, if the complete trace of Prime Network instance needs to be deleted, it is advised to use the script instead of updating the DCPL property.

- configurePN.sh [-p] <prop-file>

  This provides an option for the user to use a property file as an input to the script for copying and importing the certificates from the configured Prime Network Gateways but it doesn't update the gateway details.

  Format of the property file

  pnGatewayConfig=PN-HOSTNAME, PN_INSTALLATION_DIRECTORY, PN_SERVER_USERNAME, PN_SERVER_PASSWORD

```
pnGatewayConfig=pn1,/export/home/ana1,root,test123
pnGatewayConfig=pn2,/export/home/ana2,root,test123
```

Note It is recommended to delete the properties file after executing the script as this exposes the server credentials in plain text.

- configurePN.sh [-r]

Executing the script with this option provides a report of the gateways configured and whether the certificate from the gateway is configured or not.

Step 3 To import the certificate from Prime Network, enter **Yes** and specify the server details where the Prime Network is installed.

Uninstalling Prime Provisioning

Note It is advised to uninstall using the same user who performed the installation of Prime Provisioning.

If you attempt to uninstall Prime Provisioning as **root**, but **root** is not the Prime Provisioning owner, if you attempt to use the **./prime.sh stop** command to halt all Prime Provisioning processes, the processes will remain running. If you did not install as **root,** use the **./prime.sh stop** command before following the next steps, but be sure to execute **./prime.sh stop** *only* as the Prime Provisioning owner.

If you installed as **root**, files were created to automatically restart Prime Provisioning when rebooting the server. To remove these files, uninstall Prime Provisioning as **root**.

Next, uninstall the server, as follows:

Step 1 Log into the server.

Step 2 At the Linux prompt, log in as the identified Linux user.

Step 3 Go to the Prime Provisioning installation directory.

Step 4 Remove Prime Provisioning by entering the following command from a location outside the <*PRIMEF_HOME directory*>:

```
<PRIMEF_HOME directory>/bin/uninstall.sh
```

This command removes all files from the installation directory. This command also removes the database and its contents. Database backups are not removed if they reside in a different directory from the installation directory.