CHAPTER 23

Maintaining System Health

This chapter contains the following sections:

Monitoring System Health

To view the system health dashboards, choose **Administration > Admin Dashboard**. Table 23-1 describes the information displayed on the dashboards.

Table 23-1 **Administration > Admin Dashboard Information**

Health Information Displayed	Description
System Health	Displays memory and CPU health information over a period of time.
System Events	Displays a list of events, time the event occurred, and the severity of the event.
System Information	Displays general system health information such as the server name, number of jobs scheduled and running, the number of supported MIB variables, number of users logged in, etc.

Using System Logs

Prime Infrastructure logs all error, informational, and trace messages generated by all devices that are managed by Prime Infrastructure.

Prime Infrastructure also logs all SNMP messages and Syslogs it receives.

You can download and email the logs to use for troubleshooting Prime Infrastructure.

Step 1 Choose **Administration > Logging**. The General Logging Options Screen appears.

Step 2 Choose a Message Level.

Step 3 Check the check boxes within the Enable Log Module option to enable various administration modules. Check the **Log Modules** option to select all modules.

Step 4 In the Log File Settings portion, enter the following settings. These settings will be effective after restarting Prime Infrastructure.

Note The log file prefix can include the characters "%g" to sequentially number of files.

Step 5 Click the Download button to download the log file to your local machine.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the zip file is an html file that documents the log files.

Step 6 Enter the Email ID or Email IDs separated by commas to send the log file.

Note To send the log file in a mail you must have Email Server Configured.

Step 7 Click **Submit**.

Changing Syslog Logging Options

Step 1 Choose **Administration > Logging**, then click Syslog Logging Options.

Step 2 Check the **Enable Syslog** check box to enable collecting and processing system logs.

Step 3 Enter the Syslog Host IP address of the interface from which the message is to be transmitted.

Step 4 Choose the **Syslog Facility**. You can choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.

Step 5 Click **Save**.

Customizing Logging Options to Enhance Troubleshooting

The logging screen allows you to customize the amount of data Prime Infrastructure collects in order to debug an issue. For easily reproduced issues, follow these steps prior to contacting TAC. These steps may create a smoother troubleshooting session:

Step 1 Choose **Administration > Logging**.

Step 2 From the Message Level drop-down list, choose **Trace**.

Step 3 Check each check box to enable all log modules.

Step 4 Reproduce the current problem.

Step 5 Return to the Logging Options page.

Step 6 Click **Download** from the Download Log File section.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the zip file is an html file that documents the log files.

Step 7 After you have retrieved the logs, choose **Information** from the Message Level drop-down list.

Caution Leaving the Message Level at *Trace* can adversely affect performance over a long period of time.

Changing Global Prime Infrastructure Settings

This should be the landing page for the Administration > System Settings screen. Table needs extensive updating for all the new options on it.

Use the menu options under the Prime Infrastructure **Administration > System** menu path whenever you need to change settings that affect the product's basic behaviors. You will want to customize many of these settings when you are first implmenting Prime Infrastructure, but once in production, change them only rarely.

Table 16-3 lists the types of settings you can change using these menu options, and the detailed procedures in this User Guide that explain their effects and how to change them.

Table 23-2 Prime Infrastructure Global Settings

To do this:	Choose Administration > System Settings > ...	And:
Change which alarms, events and syslogs are deleted, and how often.	**Alarms and Events**	See Controlling Alarm, Event, and Syslog Retention, page 16-1
Set the alarm types for which email notifications are sent, and how often they are sent.	**Alarms and Events**	See Customizing Alarm Email Notifications
Set the alarm types displayed in the Alarm Summary view.	**Alarms and Events**	See Customizing Alarm Display Settings, page 23-8.
Change the content of alarm notifications sent by email.	**Alarms and Events**	See Customizing Alarm Email Content, page 23-7
Choose whehter audit logs are basic or template based.	**Audit**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Select the device parameters to audit on.	**Audit**	[Need link to one or more workflows, or one step procedure as with login disclaimer]

Table 23-2 Prime Infrastructure Global Settings (continued)

To do this:	Choose Administration > System Settings > ...	And:
Enable atuomatic troubleshooting of clients on the diagnostic channel	**Client**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Enable lookup of client host names from DNS servers and set how long to cache them	**Client**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Set how long to retain dissassociated clients and their session data	**Client**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Poll clients to identify their sessions only when a trap or syslog is received	**Client**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Disable saving of client association and dissassociation traps and syslogs as events	**Client**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Eanble saving of client authentication failure traps as events, and how long between failure traps to save them.	**Client**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Set the protocol to be used for controller and autonomous AP CLI sessions,	**CLI Session**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Enable autonomous AP migration analysis on discovery	**CLI Session**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Enable auto refresh after a wireless controller upgrade, and process the save configuration trap.	**Controller Upgrade Settings**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Set the retention period for the following data types: Trends, Device Health, Performance, Network Audit, System Health	**Data Retention**	See Scaling the System, page 16-1
Enable or disable data deduplication	**Data Deduplication**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
[Need description]	**Guest Account Settings**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Change the disclaimer text displayed at the bottom of the login page for all users.	**Login disclaimer**	Enter the login disclaimer text and click **Save**.
Enable email distribution of reports and alarm notifications.	**Mail server configuration**	See Configuring the Mail Server, page 23-6

Table 23-2 Prime Infrastructure Global Settings (continued)

To do this:	Choose Administration > System Settings > ...	And:
Configure remote event and alarm receivers who will receive notifications from Prime Infrastructure. [Following note belongs in a workflow explaining how to set thsse parms: Alerts and events are sent as SNMPv2 notifications to configured notification receivers. Note If you are adding a notification receiver with the notification type UDP, the receiver you add should be listening to UDP on the same port on which it is configured. By default only INFO level events are processed for the selected category. Only SNMPV2 traps are considered for northbound notification.]	**Notification receivers**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Configure proxies for the Prime Infrastructure server and its local authentication server.	**Proxy Settings**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Set the path where scheduled reports are stored and how long reports are retained.	**Report**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Configure the FTP, TFTP, HTTP, HTTPs, and NTP servers used.	**Server settings**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Set the severity level of any generated alarm.	**Severity Configuration**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Set the SNMP credentials and trace parameters to be used in tracing Rogue AP switch ports.	**SNMP Credentials**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Set global SNMP polling parameters, including trace display values, reachability parameters and the backoff algorithm.[Following note belongs in a section describing when and how to set these parameters: If you select Exponential (the default value) for the Backoff Algorithm, each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time. If you select to use reachability parameters, the Prime Infrastructure defaults to the global Reachability Retries and Timeout that you configure. If unchecked, Prime Infrastructure always uses the timeout and retries specified. The default is selected.]	**SNMP Settings**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Set basic and advanced swtich port trace parameters	**Switch Port Trace**	[Need link to one or more workflows, or one step procedure as with login disclaimer]

Table 23-2 Prime Infrastructure Global Settings (continued)

To do this:	Choose Administration > System Settings > ...	And:
Configure global preference parameters for downloading, distributing, and recommending software Images.	**Image Management**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Set basic control parameters used when deploying a device configuration, such as enabling backup of the running configuration, rollbacks, retrieval of show command output from cache, and the number of CLI thread pools to use.	**Configuration**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Set basic parameters for the configuration archive, such as protocol, timeout value, number of configuration versions to store, etc.	**Configuration Archive**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
[Need description]	**Audit Log Purge Settings**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
Enable automatic collection of device and interface health data, and deduplication of data on server health.	**Monitoring Settings**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
[Need description]	**Server Tuning**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
[Need description]	**User Defined OUI**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
[Need description]	**Upload OUI**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
[Need description]	**Rogue AP Settings**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
[Need description]	**Support Request Setting**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
[Need description]	**Known Ethernet MAC Address List**	[Need link to one or more workflows, or one step procedure as with login disclaimer]
[Need description]	**Port Types for Groups**	[Need link to one or more workflows, or one step procedure as with login disclaimer]

Configuring the Mail Server

Prime Infrastructure can send reports and alarm notifications via SMTP email. To enable this functionality, you must first configure one or more SMTP email servers.

Once you have configured the server, you will want to customize your reports and alarm categories to use the function and ensure that the emails are reaching the correct people.

Step 1 Select **Administration > System Settings**.

Step 2 Select **Mail Server Configuration.**

Step 3 Specify at least the following:

- The primary SMTP mail server hostname or IP address, and port,
- The sender's email address . By default, this is `NCS@Address`, where `Address` is the IP address or host name of the Prime Infrastructure server.
- A comma-separated list of one or more recipent email addresses.

Step 4 Optionally, you may also specify:

- A secondary email server. hostname or IP address, and port.
- Logon server usernames and passwords for the primary and secondary SMTP mail servers.
- Text to be appended to the subject line of every email.
- Whether you want the list of reipients you have specified to receive all alarm emails. If you enable this option, these receipients will be appended to the "To" line of every alarm email the system generates, in addition to any recipients you specified for individual alarm categories and severities..

Step 5 Click **Test** to test the mail server(s). Make corrections to the configuration as needed.

Step 6 When you are finished, click **Save**.

Related Topics

- Customizing Alarm Email Notifications, page 16-10

Customizing Alarm Email Content

By default, alarm email notificatons include only the alarm severity and alarm category in the subject line . The body of the email will contain the complete detail for the alarm.

You can customize the content of alarm notifications sent via email. You can:

- Choos e to include the alarm's severity, category, or prior alarm severity in the subject line of the email notification.
- Specify custom text to include in the subject line or body of the email notifcation.
- Replace the email subject line with the specified custom text.
- Include the current alarm condition or a link to the alarm details (instead of the text of the alarm detail) in the body of the email notification.
- Mask IP addresses and controller names in the body of the email.

These global settings apply to all alarm notifications sent by email.

Note You cannot send alarm emails unless a mail server is configured.

Step 1 Select **Administration > System Settings**.

Step 2 Select **Alarms and Events**

Step 3 Under **Alarm Email Options**, make changes as needed.

Step 4 Click **Save**.

Related Topics

- Customizing Alarm Email Notifications, page 16-10
- Customizing Alarm Display Settings, page 23-8

Customizing Alarm Display Settings

By default, the Prime Infrastructure alarm browser and other alarm lists hide all acknowledged or cleared alarms. The Alarm Display Options apply to the Alarm Summary page only. Quick searches or alarms for any entity display all alarms regardless of the acknowledged or assigned state.

You can customize how alarms are displayed using the following steps.

Step 1 Select **Administration > System Settings**.

Step 2 Select **Alarms and Events**

Step 3 Under **Alarm Display Options**, make changes as needed:

- Hide or show acknowledged alarms, assigned alarms, or cleared alarms.
- Add or remove the controller name in alarm messages
- Add or remove the Prime Infrastructure server address in all email alarm notifications

Step 4 When you are finished, click **Save**.

Related Topics

- Customizing Alarm Email Notifications, page 16-10
- Changing Alarm Status
- When to Acknowledge Alarms
- Customizing Alarm Display Settings, page 23-8

Checking the Status of Prime Infrastructure

To check the status of Prime Infrastructure from the CLI, follow these steps:

Step 1 Log into the system as **admin** by entering the following command:

```
ssh admin NCS(WAN)_server_IP address or hostname
```

Step 2 Enter the following CLI:

```
# ncs status
```

Stopping Prime Infrastructure

You can stop Prime Infrastructure at any time by following these steps:

Note If any users are logged in when you stop Prime Infrastructure, their sessions stop functioning.

Step 1 Log into the system as **admin** by entering the following command:

```
ssh admin (WAN)_server_IP address or hostname
```

Step 2 Enter the following CLI:

```
# ncs stop
```

Backing Up the Database

This section provides instructions for backing up the Prime Infrastructure database. You can schedule regular backups through the Prime Infrastructure user interface or manually initiate a backup.

Note Machine specific settings (such as FTP enable and disable, FTP port, FTP root directory, TFTP enable and disable, TFTP port, TFTP root directory, HTTP forward enable and disable, HTTP port, HTTPS port, report repository directory, and all high availability settings) are not included in the backup and restore function if the backup is restored to a different device.

This section contains the following topic:

- Scheduling Automatic Backups

Scheduling Automatic Backups

To schedule automatic backups of the Prime Infrastructure database, follow these steps:

Step 1 Log into the Prime Infrastructure user interface.

Step 2 Click **Tools > Task Manager > Background Tasks** to display the Scheduled Tasks page.

Step 3 Click the **NCS Server Backup** task to display the **NCS Server Backup** page.

Step 4 Check the **Enabled** check box.

Step 5 At the **Backup Repository** parameter, Choose an existing backup repository or click create button to create a new repository.

Step 6 If you are backing up in remote location, select the FTP Repository check box. You need to enter the FTP location, Username and Password of the remote machine.

Step 7 In the Interval (Days) text box, enter a number representing the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on.

Range: 1 to 360

Default: 7

Step 8 In the Time of Day text box, enter the time when you want the backup to start. It must be in this format: *hh*:*mm* AM/PM (for example: 03:00 AM).

Note Backing up a large database affects the performance of the Prime Infrastructure server. Therefore, we recommend that you schedule backups to run when the Prime Infrastructure server is idle (for example, in the middle of the night).

Step 9 Click **Submit** to save your settings.

The backup file is saved as a .zip file in the *ftp-install-dir*/ftp-server/root/NCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip
(for example, 10-Dec-12_10-15-22.zip).

Uninstalling Prime Infrastructure

You can uninstall Prime Infrastructure at any time, even while Prime Infrastructure is running.

To uninstall Prime Infrastructure, follow these steps:

Step 1 Log into Prime Infrastructure as **root**, then enter the following command:

```
# ncs stop
```

Step 2 Using the Linux CLI, navigate to the /opt/NCS1.0.X.X directory (or the directory chosen during installation).

Step 3 Enter **./UninstallNCS**.

Step 4 Click **Yes** to continue the uninstall process.

Step 5 Click **Finish** when the uninstall process is complete.

Note If any part of the /opt/NCS1.0.X.X directory remains on the hard drive, manually delete the directory and all of its contents. If you fail to delete the previous Prime Infrastructure installation, this error message appears when you attempt to reinstall Prime Infrastructure: "**Cisco Prime Infrastructure is already installed. Please uninstall the older version before installing this version.**"

Recovering the Prime Infrastructure Passwords

You can change the Prime Infrastructure application root user or FTP user password. This option provides a safeguard if you lose the root password. An executable was added to the installer /bin directory (passwd.bat for Windows and passwd.sh for Linux). To recover the passwords and regain access to Prime Infrastructure, follow these steps:

Note If you are a Linux user, you must be the root user to run the command.

Note In Linux, use the ***passwd.sh*** to change the Prime Infrastructure password. The ***passwd*** is a built-in Linux command to change the OS password.

Step 1 Change to the Prime Infrastructure bin folder.

Step 2 For Linux, do one of the following:

- Enter **passwd.sh root-user *newpassword*** to change the Prime Infrastructure root password. The new password is the root login password you choose.
- Enter **passwd.sh location-ftp-user *newuser newpassword*** to change the FTP user and password. The newuser and newpassword are the MSE or Location server user and password.

Step 3 The following options are available with these commands:

- -q — to quiet the output
- -pause — to pause before exiting-gui — to switch to the graphical user interface
- -force — to skip prompting for configuration

Step 4 Start Prime Infrastructure.

Downloading Device Support and Product Updates

Device Package updates and software updates for major Prime Infrastructure product releases are integrated into update bundles. These bundles are available for download directly from Cisco.

To install update bundles for Prime Infrastructure:

Step 1 Depending on your connectivity do one of the following:

- If Prime Infrastructure has external connectivity:
  - Choose **Administration > Software Update**.
  - Click **Check for Updates**.
  - Enter your Cisco.com login credentials.
- If Prime Infrastructure does not have external connectivity:
  - Go to *Cisco.com/go/ncs*.
  - Under Support, select **Download Software.**
  - Select **Cisco Prime Infrastructure** and then select the correct version of Prime Infrastructure
  - From the page that appears, download the latest update file (with the extension .ubf).

Note Be sure to download the software updates that match your Prime Infrastructure version. For example, software updates for release 1.1 can be installed only on Prime Infrastructure 1.1.

  - Choose **Administration > Software Update**.
  - Click **Upload Update File** and browse to locate the update bundles you downloaded.

The Software Updates table appears. For description of the fields see Table 1:

Table 3 Software Updates Table

Field	Description
Name	The names of software updates that have been downloaded from Cisco.com.
Published Date	Date at which the software was published to Cisco.com. The Software Updates table always shows the published dates in chronological order (oldest to most recent).
Requires Restart	If the update requires a restart, the value of this field is **yes**.
Pending Restart	If a restart is pending for the update to be complete, the value of this field is **yes**.
Installed	If the software is already installed, this field has a green check mark. If the update bundle has not yet been installed, this field is blank.
Description	To see a detailed description of the software update bundle, click the small circle to the right of the description. A dialog box appears, showing the list of patches in that update bundle

Step 2 To install the software updates:

a. Select the software updates you want to install, and click **Install**.

Note When you choose an update, all the uninstalled updates published prior to the update you have chosen are also auto-selected. In Prime Infrastructure, it is mandatory to install software updates incrementally, because older updates are sometimes prerequisites to more recent updates. This behavior also occurs in uninstallation.

The installed software updates appear at the bottom of the table, with a check mark at the **Installed** column.

b. If the **Pending Restart** value is **yes**, restart Prime Infrastructure to complete the update.

c. To uninstall any software updates, select the updates and click **Uninstall**.

Prime Infrastructure Licensing

You purchase licenses to access the Prime Infrastructure features required to manage your network. Each license also controls the number of devices or device interfaces you can manage using those features.

You need a base license and the corresponding feature licenses such as the assurance or the lifecycle license to get full access to the respective Prime Infrastructure features to manage a set number of devices or interfaces.

If you have installed Prime Infrastructure for the first time you may need an evaluation license. The evaluation license permits you to use all the features of the product to manage a limited number of devices and device interfaces for a pre defined period of time. Before the evaluation license expires, you will need to purchase the base license and the respective feature license that is sufficient to:

- Enable access to all the Prime Infrastructure features you want to use to manage your network.

- Include all the devices and interfaces in your network that you want to manage using Prime Infrastructure.

To ensure you have the licenses to achieve the above mentioned goals, follow the steps provided below:

1. Familiarize yourself with the types of license packages available to you, and their requirements. See Overview of Prime Infrastructure Licensing.
2. View the existing licenses. See Verifying License Details for help on ordering and downloading licenses.
3. Calculate the number of licenses you will need, based both on the package of features you want and the number of devices and device interfaces you need to manage. See Managing License Coverage
4. Add new licenses. See Adding Licenses.
5. Delete existing licenses. See Deleting Licenses.

If you are already using the Prime Infrastruture or any other network management product and you plan to extend your device or interface converage, see Managing License Coverage.

Overview of Prime Infrastructure Licensing

You purchase the following licenses based on the features you are required to access:

- Base License—Each Prime Infrastructure management node requires a single base license as a pre-requisite for adding feature licenses.
- Lifecycle license—The lifecycle license type is based on the number of managed devices. The lifecycle license provides full access to the Prime Infrastructure lifecycle management features. You apply for a single a base license, and then purchase life cycle licenses as necessary to accommodate additional devices. Prime Infrastructure uses a single-tier licensing structure that includes all features and functionality in one tier. Part numbers are purchased based on the number of devices to be managed. Lifecycle licenses are available in bundle sizes of 50, 100, 500, 1000, 2500, 5000, and 10000 devices and can be added together.
- Assurance license—The Assurance license is based on the number of NetFlow enabled interfaces. The Assurance license provides access to the Prime Infrastructure Assurance management features to enable you to manage a defined number of such interfaces. You apply for a single base license, and then purchase assurance licenses as necessary to accommodate additional devices. Assurance licenses are available in bundle sizes of 50, 100, 500, 1000, and 5000 devices and can be added together.
- Special PAM-15 license—The Special PAM-15 license is a stand-alone license for commerical use. You can access a maximum of 15 devices that is a combination of managed devices and NetFlow enabled interfaces after you purchase the Special PAM-15 license. If you need to add more devices or device interfaces on the network you must purchase lifecycle license or assurance license with part numbers that support 50 or more devices.

Managing License Coverage

Prime Infrastructure is deployed using physical or virtual appliances. You use the standard license center Graphical User Interface to add new licenses that is locked to the standard Cisco Unique Device Identifier (UDI). When Prime Infrastructure is deployed on a virtual appliance, the licensing is similar to that on a physical appliance, except instead of using a UDI you use a Virtual Unique Device Identifier (VUDI).

To view the UDI or VUDI, see Verifying License Details.

Note To move licenses from one physical appliance to another, you need to call the Licensing TAC and rehost the licenses to a new UDI.

If you are already using Prime Infrastructure product and need to add more devices or device interfaces follow the steps provided below.

1. Purchase add-on lifecycle or assurance licenses.
2. Apply licenses, see Adding Licenses

You can migrate to PrimeInfrastructure 1.2 if you are already using one or more of the following products.

- Prime Infrastructure 1.1
- LMS 2.x/ 3.x
- LMS 4.x
- NCS 1.0
- WCS 7.0

To migrate to Prime Infrastructure 1.2, follow the steps provided below;

1. Determine the number of licenses available for the existing product.
2. Apply for a base license and then purchase equivalent number of Prime Infrastructure upgrade licenses, see Overview of Prime Infrastructure Licensing
3. Delete existing licenses, see Deleting Licenses
4. Add new licenses, see Adding Licenses

The following table provides various examples that help you understand the licenses that you must add for unique requirements:

Table 23-4 Planning licenses

Example Scenario	Requirement
You purchase Prime Infrastructure 1.2 to manage a network consisting of 7000 devices	Add the following licenses; 1. Prime Infrastructure base license. 2. Two lifecycle licenses of device limit 5000
You are using LMS 4.0 licensed for 100 devices and need to migrate to Prime Infrastructure 1.2	1. Delete the existing license. 2. Add the following licenses: a. Prime Infrastructure base license b. Lifecycle license of device limit 100

Table 23-4 Planning licenses (continued)

Example Scenario	Requirement
You are using NCS 1.0 licensed for 600 devices and need to migrate to Prime INfrastructure 1.2 and add 100 interfaces.	1. Delete existing license. 2. Add the following licenses: a. Prime Infrastructure base license. b. Lifecycle license of device limit 500 c. Lifecycle license of device limit 100 d. Assurance license of device limit100 device interfaces
You are using LMS 4.1 licensed for 400 devices and NCS 1.0 licensed for 150 devices.	1. Delete existing licenses 2. Add the following licenses: a. Add a Prime Infrastructure base license. b. Add the lifecycle licenses of the following device limits to obtain total Prime Infrastructure entitlement: – Device limit of 300 devices and 100 devices to upgrade the LMS 4.1 licensed devices. – Device limit of 50 devices and 100 devices to upgrade the NCS 1.0 licensed devices.

Verifying License Details

To view the license type you currently have, the device and interface limits, and the percentage used and remaining on the license:

Step 1 Choose **Administration > Licenses**.

Step 2 Rest your cursor on the icon that appears next to **Licenses** to view licensing ordering help.

Adding Licenses

To add a new license:

Step 1 Choose **Administration > Licenses**.

Step 2 Under the Summary folder, click Files.

Step 3 Click **License Files**.

Step 4 Select the licenses that you have ordered with the required device limit.

Step 5 Click **Add**.

Step 6 Browse to the location of the license file, then click **OK**

Note Make sure the license file does not have a .txt extension.

Deleting Licenses

You might need to delete a license when:

- You are using an evaluation license and want to apply a base license.
- You are using a particular feature license and want to apply for a new license to accommodate additional devices.

Step 1 Choose **Administration > Licenses**.

Step 2 Under the Summary folder, click Files.

Step 3 Click **License Files**.

Step 4 Select the license file you want to delete, then click **Delete**.

Troubleshooting Licenses

You can view license information by clicking **Help > About Prime Infrastructure.**

The following table provides a few scenarios and tips for troubleshooting:

Table 23-5

Scenario	Cause	Resolution
Licensing Error	The license file becomes corrupted and unusable if you make any modifications to the file.	1. Delete the existing license. 2. Download and install a new license.
Unable to add new licenses	The base license is a pre requisite to add any additional feature license.	Install the base license
Unable to add licenses because the UDI of the device does not match.	You are adding invalid license which is not meant for that particular system.	Add the license that is ordered for the device.
The state of the devices have changed to unmanaged.	The device limit must be equal to the interface limit. The state of the inventoried devices will change to unmanaged if you add or delete devices or device interfaces. Click **Operate > Device Work Center > Collection Status** to view the status of the inventoried devices. Hover the mouse over the circle beside the device name to view the collection status details.	1. Delete the additional devices or device interfaces. 2. The state of the devices will change to managed after the 24 hours synchronisation.