CHAPTER 27

Maintaining System Health

This chapter contains the following sections:

Monitoring System Health

To view the system health dashboards, choose **Administration > Admin Dashboard**. Table 27-1 describes the information displayed on the dashboards.

Table 27-1 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. **Note** The count of internally scheduled jobs are also included in the total number of jobs displayed.

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.

Working with MSE Logs

This section describes how to configure logging options and how to download log files and contains the following topics:

Configuring Logging Options

You can use Prime Infrastructure to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to configure.

Step 3 Choose **System > Logs**. The advanced parameters for the selected mobility services engine appear.

Step 4 Choose the appropriate options from the Logging Level drop-down list.

There are four logging options: Off, Error, Information, and Trace.

All log records with a log level of Error or preceding are logged to a new error log file locserver-error-%u-%g.log. This is an additional log file maintained along with the location server locserver-%u-%g.log log file. The error log file consists of logs of Error level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.

Caution Use Error and Trace only when directed to perform so by Cisco TAC personnel.

Step 5 Select the **Enabled** check box next to each element listed in that section to begin logging its events.

Step 6 Select the **Enable** check box in the Advanced Parameters dialog box to enable advanced debugging. By default, this option is disabled.

Step 7 To download log files from the server, click **Download Logs**. See the "Downloading Mobility Services Engine Log Files" section on page 27-4 for more information.

Step 8 In the Log File group box, enter the following:

- The number of log files to be maintained in the mobility services engine. You can maintain a minimum of 5 log files and a maximum of 20 log files in the mobility services engine.
- The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.

Step 9 In the MAC Address Based Logging group box, do the following:

- Select the **Enable** check box to enable MAC address logging. By default, this option is disabled.
- Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking **Remove**.

See the "MAC Address-based Logging" section on page 27-4 for more information on MAC Address-based logging.

Step 10 Click **Save** to apply your changes.

MAC Address-based Logging

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

/opt/mse/logs/locserver

A maximum of 5 MAC addresses can be logged at a time. The Log file format for MAC address aa:bb:cc:dd:ee:ff is macaddress-debug-aa-bb-cc-dd-ee-ff.log

You can create a maximum of two log files for a MAC Address. The two log files might consist of one main and one backup or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC Address. The MAC log files that are not updated for more than 24 hours are pruned.

Downloading Mobility Services Engine Log Files

If you need to analyze mobility services engine log files, you can use Prime Infrastructure to download them to your system. Prime Infrastructure downloads a zip file containing the log files.

To download a zip file containing the log files, follow these steps:

Step 1 Choose **Services > Mobility Services**.

Step 2 Click the name of the mobility services engine to view its status.

Step 3 From the left sidebar menu, choose **Logs**.

Step 4 Click **Download Logs**.

Step 5 Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.

High Availability

To ensure continued operation in case of failure, Prime Infrastructure provides a high availability or failover framework. When an active (primary) Prime Infrastructure instance fails, a secondary Prime Infrastructure instance takes over operations. Upon failover, a peer of the failed primary Prime Infrastructure is activated on the secondary Prime Infrastructure using the local database and files, and the secondary Prime Infrastructure is fully functional. While the secondary host is in failover mode, the database and file backups of other primary Prime Infrastructure instances continue uninterrupted.

Guidelines and Limitations for High Availability

Before configuring High Availability, consider the following prerequisites and limitations:

- You must have the extra hardware identical to the primary Prime Infrastructure server to run a standby instance of Prime Infrastructure.
- Prime Infrastructure supports High Availability on both the physical and virtual appliances.
- A reliable high speed wired network must exist between the primary Prime Infrastructure instance and its backup server.
- The primary and secondary Prime Infrastructure instances must be running the same Prime Infrastructure software release.
- Failover should be considered temporary. The failed primary Prime Infrastructure instance should be restored to normal as soon as possible, and failback is reinitiated.
- The primary and secondary host are not required to share the same subnet. They can be geographically separated.
- If a secondary host fails for any reason, all the primary instances are affected, and they run in stand-alone mode without any failover support.
- The ports over which the primary and secondary Prime Infrastructure servers communicate must be open (not blocked with network firewalls, application fireways, gateways, etc.). The tomcat port is configurable during installation, and its default port is 8082. You should reserve solid database ports from 1315 to 1319.
- Any access control lists imposed between the primary and secondary Prime Infrastructure instance must allow traffic to go between the primary and secondary instances.

Failover Scenario

When a primary Prime Infrastructure instance fails, the following events take place:

1. The primary Prime Infrastructure instance is confirmed as non-functioning (hardware crash, network crash, or the like) by the health monitor on the secondary Prime Infrastructure instance.
2. If automatic failover has been enabled, Prime Infrastructure is started on the secondary as described in Step 3. If automatic failover is disabled, an e-mail is sent to the administrator asking if they want to manually start failover.
3. The secondary Prime Infrastructure server instance is started immediately (using the configuration already in place) and uses the corresponding database of the primary. After a successful failover, the client should point to the newly activated Prime Infrastructure instance (the secondary Prime Infrastructure). The secondary Prime Infrastructure instance updates all devices with its own address as the trap destination.

   Note The redirecting of web traffic to the secondary Prime Infrastructure does not occur automatically. You must use your infrastructure tools to properly configure this redirection.

4. The result of the failover operation is indicated as an event, or a critical alarm is sent to the administrator and to other Prime Infrastructure instances.

Configuring High Availability

To ensure continued operation in case of failure, you configure high availability on the primary Prime Infrastructure:

Note You must specify the Prime Infrastructure role (either standalone, primary, or secondary) during installation.

Note
- Before you configure high availability, you must configure a mail server. See the "Configuring the Mail Server" section.
- If you specify an e-mail address in the HA Configuration page then ensure a mail server is configured and reachable.

Step 1 Choose **Administration > High Availability**.

Step 2 Choose **HA Configuration** from the left sidebar menu.

Step 3 Enter the required information in the fields.

Note You must enter an e-mail address when configuring high availability. Prime Infrastructure tests the e-mail server configuration, and if the test fails (because the mail server cannot connect), the high availability configuration fails.

The default admin e-mail address that you configured in Administration > System Settings > Mail Server Configuration is automatically supplied. Any changes you make to these e-mail addresses must also be entered in the Secondary SMTP Server section of the Administration > System Settings > Mail Server Configuration page.

Step 4 Click **Save**.

Related Topics

- Guidelines and Limitations for High Availability
- Failover Scenario

Changing Global Prime Infrastructure Settings

Use the menu options under the Prime Infrastructure **Administration > System Settings** 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 implementing Prime Infrastructure, but once in production, change them only rarely.

Table 27-2 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 27-2 Prime Infrastructure Global Settings

To do this:	Choose Administration > System Settings > ...
Change which alarms, events and syslogs are deleted, and how often.	**Alarms and Events** See Controlling Background Data Collection Tasks.
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 27-11.
Change the content of alarm notifications sent by email.	**Alarms and Events** See Customizing Alarm Email Content, page 27-10.
Choose whether audit logs are basic or template based.	**Audit**
Select the device parameters to audit on.	**Audit**
Enable automatic troubleshooting of clients on the diagnostic channel	**Client**
Enable lookup of client host names from DNS servers and set how long to cache them	**Client**
Set how long to retain disassociated clients and their session data	**Client**
Poll clients to identify their sessions only when a trap or syslog is received	**Client**
Disable saving of client association and disassociation traps and syslogs as events	**Client**

Table 27-2 Prime Infrastructure Global Settings (continued)

To do this:	Choose Administration > System Settings > ...
Enable saving of client authentication failure traps as events, and how long between failure traps to save them.	**Client**
Set the protocol to be used for controller and autonomous AP CLI sessions,	**CLI Session**
Enable autonomous AP migration analysis on discovery	**CLI Session**
Enable auto refresh after a wireless controller upgrade, and process the save configuration trap.	**Controller Upgrade Settings**
Set the retention period for the following data types: Trends, Device Health, Performance, Network Audit, System Health	**Data Retention** See Scaling the System, page 26-1.
Enable or disable data deduplication	**Data Deduplication**
[Need description]	**Guest Account Settings**
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 27-9.
Configure remote event and alarm receivers who will receive notifications from Prime Infrastructure. **Note** Alerts and events are sent as SNMPv2 notifications to configured notification receivers. 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**
Configure proxies for the Prime Infrastructure server and its local authentication server.	**Proxy Settings**
Set the path where scheduled reports are stored and how long reports are retained.	**Report**
Configure the FTP, TFTP, HTTP, HTTPs, and NTP servers used.	**Server settings**
Set the severity level of any generated alarm.	**Severity Configuration**
Set the SNMP credentials and trace parameters to be used in tracing Rogue AP switch ports.	**SNMP Credentials**

Table 27-2 Prime Infrastructure Global Settings (continued)

To do this:	Choose Administration > System Settings > ...
Set global SNMP polling parameters, including trace display values, reachability parameters and the backoff algorithm. **Note** 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.	**SNMP Settings**
Set basic and advanced switch port trace parameters	**Switch Port Trace**
Configure global preference parameters for downloading, distributing, and recommending software Images.	**Image Management**
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**
Set basic parameters for the configuration archive, such as protocol, timeout value, number of configuration versions to store, etc.	**Configuration Archive**
[Need description]	**Audit Log Purge Settings**
Enable automatic collection of device and interface health data, and deduplication of data on server health.	**Monitoring Settings**

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 recipient 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 repaints you have specified to receive all alarm emails. If you enable this option, these recipients 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 Content, page 27-10

Customizing Alarm Email Content

By default, alarm email notifications 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:

- Choose 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 notification.
- 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 Topic

- Customizing Alarm Display Settings, page 27-11

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

- Changing Alarm Status, page 11-6
- When to Acknowledge Alarms, page 11-6
- Customizing Alarm Display Settings, page 27-11

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 **Administration > 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/CSCOlumos directory (or the directory chosen during installation).

Step 3 Enter **./Uninstall**.

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 27-3:

Table 27-3 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 assurance or 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 access the lifecycle and assurance features using the built-in evaluation license that is available by default. The default evaluation license is valid for 60 days for 100 devices and 150 interfaces. You can send a request to ask-prime-infrastructure@cisco.com if:

- You need to extend the evaluation period
- You need to increase the device count or interface limit
- You already have a particular feature license and need to evaluate the other feature licenses

You will need to order a base license and then purchase the corresponding feature license before the evaluation license expires. The license that you purchase must be 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 mentioned goals, do the following:

1. Familiarize yourself with the types of license packages available to you, and their requirements. See Overview of Prime Infrastructure Licensing, page 27-16.
2. View the existing licenses. See Verifying License Details, page 27-17 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, page 27-17
4. Add new licenses. See Adding Licenses, page 27-18.
5. Delete existing licenses. See Deleting Licenses, page 27-18.

If you are already using the Prime Infrastructure or any other network management product and you plan to extend your device or interface coverage, see Managing License Coverage, page 27-17.

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 prerequisite 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 following Prime Infrastructure lifecycle management features:
  - Device configuration management and archiving
  - Software image management
  - Basic health and performance monitoring
  - Troubleshooting

  You need to order a single base license, and then purchase lifecycle licenses as necessary to access the Prime Infrastructure lifecycle management features. Lifecycle licenses are available in bundle sizes of 25, 50, 100, 500, 1000, 2500, 5000, and 10000 devices and can be combined.
- Assurance license—The Assurance license is based on the number of NetFlow monitored interfaces. The Assurance license provides access to the following Prime Infrastructure Assurance management features:
  - End-to-end application, network, and end-user experience visibility
  - Multi-NAM management
  - Monitoring of WAN optimization

  You order a single base license, and then purchase assurance licenses as necessary. Assurance licenses are available in bundle sizes of 50, 100, 500, 1000, and 5000 interfaces and can be combined.

- Special Prime Assurance Manager (PAM) -15 license—The Special PAM-15 license is a stand-alone license for commercial use. This license allows you to access a maximum of 15 managed devices and NetFlow monitored interfaces, in any combination. If you need to add more devices or interfaces you must purchase additional assurance licenses with part numbers that support 50 or more interfaces.

Managing License Coverage

Prime Infrastructure is deployed using a physical or a virtual appliance. You use the standard license center GUI to add new licenses. The new licenses are locked using the standard Cisco Unique Device Identifier (UDI) for a physical appliance and a Virtual Unique Device Identifier (VUDI) for a virtual appliance.

To view the UDI or VUDI, see Verifying License Details, page 27-17.

Note To move licenses from one physical appliance to another, call the Cisco TAC and ask to have the licenses rehosted to a new UDI.

You can upgrade to Prime Infrastructure 1.2 if you are already using one or more of the following products:

- Prime Infrastructure 1.1
- NCS 1.0 (wired and wireless)
- NCS 1.1 and the corresponding maintenance releases
- WCS 7.0

For ordering information, refer to the Ordering Guide in the Prime Infrastructure Support page.

Note If you are using LMS, you need to migrate existing data from the previous installation to the new Prime Infrastructure installation.

Verifying License Details

Before you order new licenses, you might want to get details about your existing licenses. For example, you can verify your existing license type, product ID, device and interface limits, and number of devices and interfaces managed by your system.

To verify license details:

Choose **Administration > Licenses**.

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

The licensing ordering help screen that appears provides the following information:

- Feature licenses that your system is licensed for,
- Ordering options, and
- UDI or VUDI

Adding Licenses

You need to add new licenses when:

- You have purchased a new prime Infrastructure license.
- You are already using Prime Infrastructure and have bought additional licenses.
- You are upgrading to Prime Infrastructure, see Managing License Coverage, page 27-17.

To add a new license:

Step 1 Choose **Administration > Licenses**.

Step 2 Under the Summary folder, click **Files**, then click **License Files**

Step 3 Select the licenses that you have ordered with the required device limit, then click **Add.**

Step 4 Browse to the location of the license file, then click **OK.**

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.

To delete a license file:

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

To troubleshoot licenses, you will need to get details about the licenses that are installed on your system. Click **Help > About Prime Infrastructure** to access your license information.

Table 27-4 provides a few scenarios and tips for troubleshooting:

Table 27-4 Troubleshooting Scenarios

Scenario	Possible Cause	Resolution
Prime Infrastructure reports a 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 feature licenses.	The base license is a prerequisite to add any additional feature license.	1. Install the base license 2. Add new licenses
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 has 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.	1. Delete the additional devices or device interfaces. 2. The state of the devices will change to managed after the 24 hours synchronization. To verify that the status of the inventoried devices has changed to "managed" after synchronization: Choose **Operate > Device Work Center > Collection Status** Hover the mouse over the circle beside the device name to view the collection status details.

MSE Licensing Overview

The MSE packages together multiple product features related to network topology, design such as NMSP, Network Repository along with related Service Engines, and application processes, such as the following:

- Context-Aware Service
- Wireless Intrusion Prevention System (WIPS)

To enable smooth management of MSE and its services, various licenses are offered.

Note You must have a Cisco Prime Infrastructure license to use MSE and its associated services.

This section contains the following topics:

MSE License Structure Matrix

Table 27-5 lists the breakdown of the licenses between the High end, Low end and Evaluation licenses for MSE, Location services, SCM, wIPS and MIR.

Table 27-5 MSE License Structure Matrix

	High End	Low End	Evaluation
MSE Platform	High-end appliance and infrastructure platform such as the Cisco 3350 and 3355 mobility services engines.	Low-end appliance and infrastructure platform such as Cisco 3310 mobility services engine.	—
Context Aware Service	25,000 Tags	2000 Tags	Validity 60 days, 100 Tags and 100 Elements.
	25,000 Elements	2000 Elements	
wIPS	3000 access points	2000 access points	Validity 60 days, 20 access points.

Sample MSE License File

The following is a sample MSE license file:

```
FEATURE MSE cisco 1.0 permanent uncounted \
    VENDOR_STRING=UDI=udi,COUNT=1 \
    HOST ID=ANY \
    NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</LicLineID> \
    <PAK>dummyPak</PAK>" \
    SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \
    45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \
    1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

This sample file has 5 license entries. The first word of the first line of any license entry tells you what type of license it is. It can either be a Feature or Increment license. A feature license is a static lone item to license. There can be multiple services engines running in MSE. An Increment license is an additive license. In MSE, the individual service engines are treated as increment licenses.

The second word of the first line defines the specific component to be licensed. For example, MSE, LOCATION_TAG. The third word depicts the vendor of the license, for example Cisco. The fourth word denotes the version of the license, example 1.0. The fifth word denotes the expiration date, this can be permanent for licenses that never expire or a date in the format dd-mm-yyyy. The last word defines whether this license is counted.

Revoking and Reusing an MSE License

You can revoke an MSE appliance license from one system and reuse it on another system. When you revoke a license, the license file is deleted from the system. If you want to reuse the license on another system, then the license needs to be rehosted.

If you want to reuse a license with an upgrade SKU on another system, then you must have the corresponding base license SKU installed in the system to which you want to reuse the upgrade SKU. You cannot reuse the upgrade license SKU in a system if the corresponding base license SKU is deleted from it.

When you revoke a license, MSE restarts the individual service engines to reflect the changes to the licenses. Then the service engines receives the updated capacity from MSE during startup.

MSE Services Co-Existence

With MSE 6.0 and later, you can enable multiple services (Context Aware and wIPS) to run concurrently. Before Version 6.0, mobility services engines only supported one active service at a time.

The following must be considered with co-existence of multiple services:

- Co-existence of services might be impacted by license enforcement. As long as the license is not expired, you can enable multiple services.

  Note Limits for individual services differ. For example, a low-end mobility services engine (MSE-3310) tracks a total of 2,000 CAS elements; a high-end mobility services engine (MSE-3350) tracks a total of 25,000 CAS elements.
  A low-end mobility services engine has a maximum limit of 2000 wIPS elements; a high-end mobility services engine has a maximum limit of 3000 wIPS elements.

- Expired evaluation licenses prevent the service from coming up.
- If a CAS license is added or removed, this process restarts all services on the mobility services engine including wIPS. If a wIPS license is added or removed, the process does not impact CAS; only wIPS restarts.
- Other services can be enabled in evaluation mode even if a permanent license for the maximum number of elements has been applied.

Whenever one of the services has been enabled to run with its maximum license, another service cannot be enabled to run concurrently because the capacity of the MSE is not sufficient to support both services concurrently. For example, on MSE-3310, if you install a wIPS license of 2000, then you cannot enable CAS to run concurrently. However, evaluation licenses are not subject to this limitation.

Managing Mobility Services Engine (MSE) Licenses

If you choose Files > MSE Files from the left sidebar menu, you can manage the mobility services engine licenses.

This section contains the following topics:

- Registering Product Authorization Keys, page 27-22
- Installing Client and wIPS License Files, page 27-23
- Deleting a Mobility Services Engine License File, page 27-24

The page displays the mobility services engine licenses found and includes the following information:

Note Because tag licenses are added and managed using appropriate vendor applications, tag licenses are not displayed in this page. Refer to the following URL for more information: http://support.aeroscout.com.
Evaluation (demo) licenses are also not displayed.

Tag licenses are installed using the *AeroScout System Manager* only if the tags are tracked using Partner engine. Otherwise the tags will be counted along with the CAS element license.

- MSE License File—Indicates the MSE License.
- MSE—Indicates the MSE name.
- Type—Indicates the type of mobility services engine (client elements, wIPS local mode or wIPS monitor mode access points).
- Limit—Displays the total number of client elements or wIPS monitor mode access points licensed across the mobility services engine.
- License Type—Permanent licenses are the only license types displayed on this page.
  - Permanent—Licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.

Registering Product Authorization Keys

You receive a product authorization key (PAK) when you order a client, wIPS, or tag license from Cisco. You must register the PAK to receive the license file for install on the mobility services engine. License files are emailed to you after successfully registering a PAK.

Client and wIPS PAKs are registered with Cisco.

Note Tag PAKs are registered with AeroScout. To register your tag PAK, go to this URL: http://www.aeroscout.com/content/support

To register a product authoritative key (PAK) to obtain a license file for install, follow these steps:

Step 1 Open a browser page and go to www.cisco.com/go/license.

Note You can also access this site by clicking the Product License Registration link located on the License Center page of NCS.

Step 2 Enter the PAK and click **SUBMIT**.

Step 3 Verify the license purchase. Click **Continue** if correct. The licensee entry page appears.

Note If the license is incorrect, click the **TAC Service Request Tool** link to report the problem.

Step 4 At the Designate Licensee page, enter the mobility service engine UDI in the host ID text box. This is the mobility services engine on which the license will be installed.

Note UDI information for a mobility services engine is found in the General Properties group box at Services > Mobility Services Engine > *Device Name* > *System*.

Step 5 Select the **Agreement** check box. Registrant information appears beneath the Agreement check box.

Modify information as necessary.

Note Ensure that the phone number does not include any characters in the string for the registrant and end user. For example, enter 408 555 1212 rather than 408.555.1212 or 408-555-1212.

Step 6 If registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the end user information.

Step 7 Click **Continue**. A summary of entered data appears.

Step 8 At the Finish and Submit page, review registrant and end user data. Click **Edit Details** to correct information, if necessary.

Step 9 Click **Submit**. A confirmation page appears.

Installing Client and wIPS License Files

You can install CAS element licenses and wIPS licenses from Prime Infrastructure.

Note Tag licenses are installed using the *AeroScout System Manager*. Refer to the following URL for additional information:
http://support.aeroscout.com.

To add a client or wIPS license to Prime Infrastructure after registering the PAK, follow these steps:

Step 1 Choose **Administration > License Center**.

Step 2 From the left sidebar menu, choose **Files > MSE Files**.

Step 3 From the License Center > Files > MSE Files page, click **Add** to open the Add a License File dialog box.

Step 4 From the MSE Name drop-down list, choose the mobility services engine to which you want to add the license file.

Note Verify that the UDI of the selected mobility services engine matches the one you entered when registering the PAK.

Step 5 Enter the license file in the License File text box or browse to the applicable license file.

Step 6 Once displayed in the License File text box, click **Upload**. Newly added license appears in mobility services engine license file list.

Note A Context Aware Service (CAS) restarts if a client or tag license is installed; a wIPS service restarts if a wIPS license is installed.

Note Services must come up before attempting to add or delete another license.

Deleting a Mobility Services Engine License File

To delete a mobility services engine license file, follow these steps:

Step 1 From the License Center > Files > MSE Files page, select the check box of the mobility services engine license file that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm the deletion.