Overview of Cisco Prime LAN Management Solution 4.2

This chapter provides overview of LMS 4.2 and data migration from earlier versions of LMS to LMS 4.2. This chapter contains:

- Product Overview
- Install and Upgrade Behavior
- New Features and Enhancements in LMS 4.2
- Data Migration Overview
- Supported Network Management Systems
- Supported Devices

Product Overview

LMS 4.2 provides powerful features that enable you to configure, monitor, troubleshoot, and administer Cisco networks. It also supports new Cisco technologies such as Identity, EnergyWise, Auto Smartports, Medianet, and Smart Install.

This document describes procedures for new and upgrade installation of LMS 4.2. It contains:

- LMS functionalities.
- LMS features.
- Hardware and software requirements.
- Detailed installation procedures.
- Frequently asked questions.
- Information about ordering documentation and contacting Cisco Systems for additional assistance.

If you already have an earlier version of LMS and want to migrate to LMS 4.2, see Migrating Data to Cisco Prime LAN Management Solution 4.2.
The licenses in LMS 4.2 are based on number of devices and you can manage the following functionalities for the devices:

- Configuration Management (This function is enabled by default. You cannot select or unselect this function)
- Network Topology, Layer 2 Services and User Tracking
- Fault Management
- IPSLA Performance Management
- Device Performance Management

There are additional licenses available for managing performance collectors. See System and Browser Requirements for Server and Client and Application Scaling Numbers for more details.

Install and Upgrade Behavior

LMS 4.2 provides a single install experience to you. For complete details on installation, see Performing Installation of Cisco Prime LMS 4.2

Note
We recommend you not to install any other product in LMS server. If LMS 4.2 and Antivirus softwares like MCAfee, Norton and so on, are installed in the same machine, the Antivirus should be configured to exclude the NMSROOT (LMS installation directory) from scanning. This is required because the third party software such as Sybase, included in LMS do disk intensive operations and spawn child processes based on the load. If the Antivirus is enabled this may not function as expected or may cause degradation in the overall performance of LMS.

Note
Daemon Manager will start slowly during reboot. This is because the antivirus that starts during reboot will cause delay to initiate Cisco Prime processes. If there are any Daemon Manager issues during reboot, then you should either disable the antivirus or restart the Daemon Manager after reboot.

Note
After LMS 4.2.5 installation, we recommend to reboot the server as Linux kernel is upgraded.

This section contains the following topics on Upgrade:
- Overview of Upgrade and Migration
- Upgrading Master-Slave Server Setup

Overview of Upgrade and Migration

Upgrading is overwriting the existing LMS version with a new LMS version. You have to freshly install LMS 4.2 and then perform data migration.

You can upgrade using either of these methods:
- Local upgrade—Upgrading to the newer version of LMS on the same machine.
LMS 4.2 supports local upgrade or direct inline upgrade only from LMS 4.1 and LMS 4.0.1.

- Remote upgrade—Installing LMS on a different machine and then restoring the data on that machine.

You can do a remote upgrade to LMS 4.2 from LMS 4.1, LMS 4.0.1, and LMS 3.2 SP1. For earlier versions of LMS, refer Table 1-2.

### Upgrading Master-Slave Server Setup

Table 1-1 provides you details on Upgrading Master-Slave Server Setup

<table>
<thead>
<tr>
<th>Behavior Changes After Remote Upgrade</th>
<th>LMS Master</th>
<th>LMS Slave</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Migration Changes</td>
<td>After restoring the LMS 3.2 SP1/4.0.1/4.1 backed up data in LMS 4.2, the DCR mode will be moved from Standalone to Master</td>
<td>• After taking backup from LMS 3.2 SP1, install LMS 4.2, the DCR mode will be in Standalone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• After restoring the LMS 3.2 SP1/4.0.1 backed up data in LMS 4.2, the DCR mode will be in Standalone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You should change the mode to Slave</td>
</tr>
<tr>
<td>DCR Changes</td>
<td>No Changes</td>
<td>DCR devices will be deleted from Slave or pushed to Master based on your choice, and data will be synchronized from Master</td>
</tr>
<tr>
<td>Device Management/Allocation changes</td>
<td>After remote migration, the device management allocation policy will be set as it was before. For Example, if the allocation policy is set to On in LMS 3.2 SP1/4.0.1/4.1 server, after remote migration to LMS 4.2 the same settings will be retained.</td>
<td>Device management allocation policy is set to Off, and all the devices will be moved to unmanaged state. This allows you to decide in managing devices in the Slave</td>
</tr>
<tr>
<td>Grouping Services Changes</td>
<td>User-defined groups in Slave will not be shared or synchronized with Master in LMS 4.2</td>
<td>User-defined groups can be created in LMS 4.2 Slave as against previous releases like LMS 3.2 SP1 and above. User-defined groups created in Master is shared in Slave server.</td>
</tr>
<tr>
<td></td>
<td>• Exporting of groups from Slave and importing to Master is possible.</td>
<td>• Exporting of groups from Master and importing to Slave is possible</td>
</tr>
<tr>
<td></td>
<td>• Grouping services might not work if Master or Slave has different versions of LMS. We recommend you to use the same LMS version across all servers in DCR management domain.</td>
<td>• System defined (device type) groups are separately created in Slave</td>
</tr>
</tbody>
</table>
Table 1-2 describes the recommended sequence to upgrade, and migrate your data from earlier versions of LMS to LMS 4.2.

### Table 1-2 Upgrade and Data Migration Procedure

<table>
<thead>
<tr>
<th>Current LMS Version</th>
<th>Type of Upgrade</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMS 4.1</td>
<td>Remote migration</td>
<td>1. Back up the data in the old machine having LMS 4.1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Install LMS 4.2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Migrate your data to LMS 4.2 using the instructions explained in the section Remote Upgrade to LMS 4.2.</td>
</tr>
<tr>
<td></td>
<td>Direct inline migration</td>
<td>1. Install LMS 4.2 over LMS 4.1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The data is automatically migrated during installation.</td>
</tr>
<tr>
<td>LMS 4.0.1</td>
<td>Remote migration</td>
<td>1. Back up the data in the old machine having LMS 4.0.1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Install LMS 4.2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Migrate your data to LMS 4.2 using the instructions explained in the section Remote Upgrade to LMS 4.2.</td>
</tr>
<tr>
<td></td>
<td>Direct inline migration</td>
<td>1. Install LMS 4.2 over LMS 4.0.1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The data is automatically migrated during installation.</td>
</tr>
<tr>
<td>LMS 3.2 SP1</td>
<td>Remote migration</td>
<td>1. Back up the data in the old machine having LMS 3.2 SP1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Install LMS 4.2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Migrate your data to LMS 4.2 using the instructions explained in the section Remote Upgrade to LMS 4.2.</td>
</tr>
</tbody>
</table>
## Upgrade and Data Migration Procedure

<table>
<thead>
<tr>
<th>Current LMS Version</th>
<th>Type of Upgrade</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMS 2.6, LMS 2.6 SP1, LMS 3.0, LMS 3.0 December 2007 update, LMS 3.1</td>
<td>Remote migration</td>
<td>1. Back up the data in the old machine.</td>
</tr>
<tr>
<td></td>
<td>Direct inline upgrade to LMS 4.2 is not supported.</td>
<td>2. Install LMS 4.0.1 in the new machine.</td>
</tr>
<tr>
<td></td>
<td>The suggested upgrade path is: LMS 2.6/LMS 2.6 SP1/LMS 3.0/LMS 3.0 December 2007 update/LMS 3.1 &gt; LMS 3.2 &gt; LMS 4.0 &gt; LMS 4.0.1 &gt; LMS 4.2</td>
<td>3. Migrate the data to LMS 4.0.1. For more information, see <a href="http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/install/guide/dmg.html">http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/install/guide/dmg.html</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Install LMS 4.2.</td>
</tr>
<tr>
<td></td>
<td>From LMS 4.0.1 to LMS 4.2, you can perform direct inline or remote upgrade, click <a href="http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/install/guide/dmg.html">here</a> for more details.</td>
<td></td>
</tr>
<tr>
<td>LMS 2.2, LMS 2.5, LMS 2.5.1</td>
<td>Remote migration</td>
<td>1. Back up the data in the old machine.</td>
</tr>
<tr>
<td></td>
<td>Direct inline upgrade to LMS 4.2 is not supported.</td>
<td>2. Upgrade from the earlier versions of LMS to LMS 2.6 and migrate the data, using the instructions in:</td>
</tr>
<tr>
<td></td>
<td>The suggested upgrade path is: LMS 2.2 / LMS 2.5 / LMS 2.5.1 &gt; LMS 2.6 &gt; LMS 4.0 &gt; LMS 4.0.1 &gt; LMS 4.2</td>
<td>- <a href="http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/2.6/lan_management_solution/2.6.html">Readme for CiscoWorks LMS 2.6 Update on Solaris</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Install LMS 4.0.1 in the new machine.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Migrate the data to LMS 4.0.1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Install LMS 4.2.</td>
</tr>
<tr>
<td></td>
<td>From LMS 4.0.1 to LMS 4.2, you can perform direct inline or remote upgrade, click <a href="http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/install/guide/dmg.html">here</a> for more details.</td>
<td></td>
</tr>
</tbody>
</table>
New Features and Enhancements in LMS 4.2

This section explains the new features in LMS 4.2.
See the Online help of LMS 4.2 applications for a detailed explanation on new features in LMS 4.2.
This section contains the following:

- Creating Configuration Templates
- Idle Timeout Settings
- Standard Discovery
- CAAM Features
- Hardware Configuration-based MIB Objects Polling
- Poller Management Enhancements
- Troubleshooting Workflow Changes
- Fault Management Generic Device Package Support and Traps Support
- Enhancement in Unused POE Report
- Enhancement in Custom Inventory Report
- Enhancement in TrustSec
- EnergyWise Enhancement
- Report Designer Enhancement
- VLAN Fetch Support for SCP and RCP
- Template Center Enhancement
- Third-Party Software and Tool Changes

Note

The supported screen resolution for LMS 4.2 is 1024x768 pixels. We recommend you not to use browser zoom in and zoom out features in LMS 4.2.

Creating Configuration Templates

CLI templates are user-defined templates that are created based on your own parameters. CLI templates allow you to choose the elements in the configurations. LMS provides variables that you replace with actual values and logic statements.
For more information, see Creating Configuration Templates in Configuration Management with Cisco Prime LAN Management Solution 4.2.

Idle Timeout Settings

If UI is kept idle for the set time period then a pop-up redirecting the page to idle page will be displayed. You can click cancel to avoid redirecting to the idle page.
If you are redirected to the idle page then click click here link to return to your previous page. The default idle timeout is 120 minutes.
Standard Discovery

Standard Discovery allows you to discover devices with minimum settings. For configuring Standard Discovery, you need to provide the input for Seed Devices and SNMP Credentials.

Inputs for seed device can be given as follows:
- Using default gateway as seed, this option is chosen by default
- Using Seed devices from DCR, it will not show the count of devices in DCR
- Providing Seed devices manually in TextArea separated by space

Inputs for SNMP credentials can be given as follows:
- Use Policy Configuration
- Custom Policy Configuration
- Default set credentials
- Provide Credentials Manually

For more information, see Inventory Management with Cisco Prime LAN Management Solution 4.2.

CAAM Features

LMS 4.2 supports the following Compliance and Audit Manager (CAAM) features:
- Data Synchronization between LMS and CAAM
- Managing Policy Groups
- Managing Policy Profile
- Fixing Profile Violation
- Compliance Data Collection
- Import Contracts
- CAAM Reports
- CAAM Offline Update
- CAAM Online Update

Data Synchronization between LMS and CAAM

CAAM database should always be in sync with LMS database. When a new device is added to LMS or an unmanaged device is managed, and if the CAAMServer process is down, the device will not be added to CAAM database. When the CAAMServer process comes up, the device will be added to CAAM database but the device details such as Inventory, Config and Show Commands will not be updated in CAAM database. You have to manually perform Inventory, Config, and Show Commands collection to update the CAAM database.

For more information, see Using Compliance and Audit Manager Feature in Configuration Management with Cisco Prime LAN Management Solution 4.2.
Chapter 1  Overview of Cisco Prime LAN Management Solution 4.2

Managing Policy Groups

Policy Group is a collection of Policies. Policies are defined by a set of rules. LMS 4.2 supports 293 policies. In addition to the system-defined Policy Groups, you can create your own Policy Groups by selecting a set of system-defined policies. LMS allows you to add, clone, edit, and delete policy groups.

For more information, see Using Compliance and Audit Manager Feature in Configuration Management with Cisco Prime LAN Management Solution 4.2.

Managing Policy Profile

Policy Profile is a set of Policy Groups where each Policy Groups are mapped with set of devices/device groups. LMS allows you to add, clone, edit, and delete policy profile. It also allows you to run the compliance check and view the job history.

For more information, see Using Compliance and Audit Manager Feature in Configuration Management with Cisco Prime LAN Management Solution 4.2.

Fixing Profile Violation

The Profile Violations Fix Report lists all the devices that do not comply with a defined user profile. A profile is defined as a policy or a set of policies applied on either a device or a set of devices. LMS provides configuration commands for fixing the violation.

For more information, see Using Compliance and Audit Manager Feature in Configuration Management with Cisco Prime LAN Management Solution 4.2.

Compliance Data Collection

This feature allows you to schedule the Compliance Data Collection System Job. The Compliance Data Collection job runs daily by default.

For more information, see Compliance and Audit Settings in Administration of Cisco Prime LAN Management Solution 4.2.

CAAM Offline Update

This feature allows you to download and install the patches related to CAAM Server manually.

For more information, see Compliance and Audit Settings in Administration of Cisco Prime LAN Management Solution 4.2.

CAAM Online Update

Enables you to download and install the patches related to CAAM Server online.

For more information, see Compliance and Audit Settings in Administration of Cisco Prime LAN Management Solution 4.2.

Import Contracts

This feature enables you to import customer contracts into the CAAM Database.
For more information, see Compliance and Audit Settings in *Administration of Cisco Prime LAN Management Solution 4.2*.

**CAAM Reports**

CAAM reports provide compliance status of the network, lifecycle and contract information about network devices, security advisory, and service reports based on device and software capabilities, and the services that are enabled.

Using CAAM, the following reports can be generated and viewed in the reports job browser:

- Service Reports
- Life Cycle Management Reports
- Compliance Reports

For more information, see Compliance and Audit in *Reports Management with Cisco Prime LAN Management Solution 4.2*.

**Service Reports**

Service reports provide information about the status of all the services on network nodes. These reports also include a Capability Report section that provides information on what a user needs to do like upgrading the software or hardware for supporting a given service.

**Life Cycle Management Reports**

Life Cycle Management Reports provide information about the lifecycle state of the network. This report includes End of Life and Contract Management Reports.

**Compliance Reports**

The Compliance Reports provide information about the compliance state of the network for specific compliance requirements.

Compliance Reports include the following device reports:

- HIPAA Compliance Reports
- SOX (COBIT) Compliance Report
- ISO/IEC 27002 Compliance Reports
- NSA Compliance Reports
- PCI DSS Compliance Reports
- DHS Checklist Reports
- DISA Checklists Report
- CIS Benchmarks
- Vendor Advisory Reports

**Hardware Configuration-based MIB Objects Polling**

When LMS server with specific hardware configuration polls MIB objects more than the recommended number, a warning message is displayed.

For more information, see Hardware Configuration-based MIB Object Polling Support in *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2*. 
Poller Management Enhancements

In this release, Poller Management UI displays the polling preference types namely, Poll All Instances, Poll by Pattern, and Poll by User Selection. Poll by Pattern is a new polling preference type introduced in this release.

For more information, see Creating a Poller in Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2.

Troubleshooting Workflow Changes

Device Information portlet in the Device Troubleshooting workflow is enhanced and it displays additional information such as CPU Utilization, Memory Utilization and so on.

For more information, see Device Information in Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2.

Fault Management Generic Device Package Support and Traps Support

In this release, LMS Fault Management functionality supports unknown devices and non-Cisco devices with limited functionalities.

Unknown devices here refer to Cisco devices for which device package updates are not installed and available on LMS server.

Unknown devices and non-Cisco devices together referred as Generic devices in LMS.

For more information, see Understanding the Detailed Device View in Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2.

In this release, Trap support is provided for SNMPv3 configured devices, SNMPv2 configured devices, unknown devices, and non-Cisco devices.

For more information, see Configuring SNMP Trap Receiving and Forwarding in Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.2.

Enhancement in Unused POE Report

You can view an unused PoE report with detailed information of PoE-enabled devices managed by LMS along with the information of the ports that are not connected to the end points.

For more information, see Generating an Unused PoE Report in Reports Management with Cisco Prime LAN Management Solution 4.2.

Enhancement in Custom Inventory Report

New Inventory Groups are added and few attributes have been added to the existing Inventory Groups.
Chapter 1      Overview of Cisco Prime LAN Management Solution 4.2

New Features and Enhancements in LMS 4.2

For more information, see Creating an Inventory Custom Report Template in Reports Management with Cisco Prime LAN Management Solution 4.2.

Enhancement in TrustSec

Till LMS 4.1, Identity was a separate feature. In LMS 4.2, Identity, which is now called as 802.1x, and Secured Group Access Configuration (SXP, SGT, and SGACL) are grouped under a common feature called TrustSec.

TrustSec Version

When you launch the Getting Started/Readiness Assessment page from Work Centers > TrustSec > Getting Started/Readiness Assessment for the first time, you will be guided to select the TrustSec version (TrustSec 1.99 and TrustSec 2.0) inorder to list the TrustSec-capable devices. By default TrustSec 2.0 is selected.

TrustSec Limited Compatibility Devices

In the TrustSec Getting Started/Readiness Assessment page, the pie chart is enhanced with TrustSec Limited Compatibility Devices. If devices are running with minimum supported image version for the selected TrustSec version and if the devices are not having the required modules installed then those devices will be known as TrustSec Limited Compatibility devices.

For more information, see TrustSec Readiness Assessment in Technology Work Centers in Cisco Prime LAN Management Solution 4.2.

<table>
<thead>
<tr>
<th>Inventory Group</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge</td>
<td>Base Bridge Address</td>
</tr>
<tr>
<td></td>
<td>Number of Ports</td>
</tr>
<tr>
<td></td>
<td>Bridge Type</td>
</tr>
<tr>
<td>Container</td>
<td>Container Model Name</td>
</tr>
<tr>
<td></td>
<td>Container Vendor Type</td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>Manufacturer Name</td>
</tr>
<tr>
<td></td>
<td>Physical Entity Name</td>
</tr>
<tr>
<td>Interface</td>
<td>interface index</td>
</tr>
<tr>
<td>Memory pool</td>
<td>Lowest Free Block (MB)</td>
</tr>
<tr>
<td>Module</td>
<td>Slot Number</td>
</tr>
<tr>
<td>Port</td>
<td>Port Index</td>
</tr>
<tr>
<td></td>
<td>Port Description</td>
</tr>
<tr>
<td></td>
<td>Port Vendor Type</td>
</tr>
<tr>
<td>System</td>
<td>Management Type</td>
</tr>
<tr>
<td></td>
<td>OSI Layer Services</td>
</tr>
</tbody>
</table>

For more information, see Creating an Inventory Custom Report Template in Reports Management with Cisco Prime LAN Management Solution 4.2.
Secured Group Access Configuration

Secured Group Access Configuration cross-launches the Template Center page, where you can select the template and deploy configuration.

This can be done in two ways:

- Go to Work Centers > TrustSec > Getting Started or Readiness Assessment, select the devices from the TrustSec-capable devices pie or TrustSec Limited Compatibility pie and click SXP, SGT, or SGACL Configure options.

  or

- Go to Work Centers > TrustSec > Secured Group Access Configuration select the devices and click SXP, SGT, or SGACL Configure options.

For more information, see Secured Group Access Configuration in Technology Work Centers in Cisco Prime LAN Management Solution 4.2.

EnergyWise Enhancement

In the EnergyWise Policy Override portlet, Wake the host option is newly added.

In the Current Power Consumption portlet, a new field “Category” has been added.

In the Work Center > EnergyWise > Configure > Manage Endpoint Groups flow, a new field “Category” has been added.

For more information, see Technology Work Centers in Cisco Prime LAN Management Solution 4.2.

Report Designer Enhancement

Earlier, Syslog and Inventory Custom Report templates were combined as a single workflow. In LMS 4.2, Syslog and Inventory Custom Report are available as two separate flows.

For more information, see Report Designer in Reports Management with Cisco Prime LAN Management Solution 4.2.

In the Inventory Custom Report template, Report Attributes and Rules for Attributes are available as two different sections, where the generated report will display only the attributes selected under Report Attributes section.

For more information, see Creating Inventory Custom Reports in Reports Management with Cisco Prime LAN Management Solution 4.2.

VLAN Fetch Support for SCP and RCP

You can set the protocol order for Configuration Management features such as Archive Management, Config Editor, and NetConfig jobs to download configurations and to fetch configurations. For NetShow and VLAN Fetch, you can set the protocol order to download configurations.

For more information, see Configuring Transport Protocols in Administration of Cisco Prime LAN Management Solution 4.2.
Template Center Enhancement

In LMS 4.2, you can create Configuration templates using IF and FOREACH statements.
For more information, see Guidelines for Creating Configuration Templates Using IF and FOREACH Statements in Configuration Management with Cisco Prime LAN Management Solution 4.2.

Third-Party Software and Tool Changes

The following are the changes in the third-party software and tools in this release:

- Support for Windows 2012 Standard Edition and Data Center Edition on server and client systems

Note For Windows 2012 support, install LMS 4.2 using CiscoPrime_LMS_4.2_WIN12.exe file and then upgrade to LMS 4.2.5 by following the conventional installation steps.

- WinPcap upgrade to 4.0.2
- Daylight Savings Timezone tool upgrade to 1.3.45-b01
- Firefox 8.0 and 9.0 support on client systems
- Java Plug-in version 1.6.0_24 or later update versions only
- Apache upgrade to 2.2.17
- Java Runtime Environment (JRE) 1.6.0_24

Data Migration Overview

You can freshly install LMS 4.2 and then perform remote data migration. LMS 4.2 supports direct inline upgrade from LMS 4.1, and LMS 4.0.1.

Data Migration to LMS 4.2 can be done using the following methods:

- Normal Backup - Process by which all the configuration files and collected data can be backed up from application database.
- Selective Backup - Process by which only required system configurations and data can be backed up.

The following migration paths are available for the customers.

- LMS 4.1
- LMS 4.0.1
- LMS 3.2 SP1

For the following versions, you must migrate to LMS 3.2 SP1, and then install LMS 4.2:

- LMS 3.1
- LMS 3.0 Dec 2007 update
- LMS 3.0
- LMS 2.6 SP1
Supported Network Management Systems

- LMS 2.6

Note

LMS 3.2 and earlier versions allow you to install partial applications in one server. For example, you can install CS and RME (part of earlier LMS versions) in one server and other LMS applications in another server. In this scenario you can perform data migration only from one server. You can migrate data either from RME server or from another LMS server. If the migration is performed from both the servers, then the last run migration will overwrite the previously migrated data.

See Migrating Data to Cisco Prime LAN Management Solution 4.2 for more details on data migration.

**Supported Network Management Systems**

Table 1-3 lists the Network Management Systems (NMS) supported by Integration Utility 1.11, which is part of LMS 4.2.

Note

HPOV or NetView adapters are not supported for the Fault Management functionality in LMS 4.2

See Importing From Remote NMS in the Inventory Management Online Help for information about importing devices from third party NMS.

Network Management Integration Data Bundle (NMIDB) 1.0.089 is shipped with LMS 4.2.

Note

From HPOV 9.x onwards the integration utility is moved to HPOV software.

For more information about HP NNMi and Cisco Prime LMS Integration, refer the User Guide for Integration Utility 1.11 on Cisco.com.
### Table 1-3 Supported Network Management Systems

<table>
<thead>
<tr>
<th>Network Management System</th>
<th>Supported Platforms</th>
</tr>
</thead>
</table>
| HP OpenView 9.1, 9.01, 9.0, 8.13, 8.1 | **Windows**  
- Windows 2008 R2 Standard x 64 Edition  
- Windows 2008 Server Standard Edition Release 1 with SP1 and SP2  
- Windows 2008 Enterprise Edition Release 1 with SP1 and SP2  
- Windows Server 2008 R2 Standard Edition  
- Windows Server 2008 R2 Enterprise Edition  
**Note** Note Only 64-bit Operating Systems are supported on the above versions. |
|                           | **Solaris**  
- Solaris 10  
Both local and remote integration are supported for these platforms. |
|                           | **Soft Appliance**  
**Note** Only remote integration is supported for Soft Appliance.  
For information on integrating HP OpenView- LMS, see NNMi Deployment Guide on the HP site. |
<table>
<thead>
<tr>
<th>Network Management System</th>
<th>Supported Platforms</th>
</tr>
</thead>
</table>
| HP OpenView 7.53, 7.51, 7.50 | **Windows:**  
  - Windows 2008 Server Standard Edition Release 1 with SP1 and SP2  
  - Windows 2008 Enterprise Edition Release 1 with SP1 and SP2  
  - Windows Server 2008 R2 Standard Edition  
  - Windows Server 2008 R2 Enterprise Edition  
  **Note** Only 64-bit Operating Systems are supported on the above versions.  
| Solaris |  
  - Solaris 10  
  Only remote integration is supported for the above platforms.  
| NetView 7.1.4, 7.1.5 | **Windows:**  
  - Windows 2008 Server Standard Edition Release 1 with SP1 and SP2  
  - Windows 2008 Enterprise Edition Release 1 with SP1 and SP2  
  - Windows Server 2008 R2 Standard Edition  
  - Windows Server 2008 R2 Enterprise Edition  
  **Note** Only 64-bit Operating Systems are supported on the above platforms.  
|              | Only remote integration is supported for the above platforms.  |
Supported Devices

As additional device packages become available, you can download the Service Packs (formerly called IDUs) that contain them from Cisco.com.

Registered Cisco.com users can access the latest Device Package Updates, and download the latest device updates for CiscoView, Topology Device Package Updates, Fault Management Device Package Updates and Inventory Config And Image Management Device Package Updates from:


See the following documentation to know more information about supported devices:

- Supported Devices Table for Cisco Prime LAN Management Solution 4.2
- User Guide for CiscoView 6.1.9
  CiscoView manages and configures different types of Cisco devices. You can refer this document for information on supported devices. This document is available on Cisco.com at this URL:

To see the list of installed application’s device packages, select **Admin > System > Software Center > Device Update** from the LMS menu.

To download Device Package Updates:

**Step 1**
Go to http://www.cisco.com/cisco/software/type.html?mdfid=283434800&flowid=19062

You must be a registered Cisco.com user to access this Software Download site. The site prompts you to enter your Cisco.com username and password in the login screen, if you have not logged in already.

**Step 2**
Select the Software Product Category as **Cloud and Systems Management**.

**Step 3**
Select **Routing and Switching Management > Cisco Prime LAN Management Solution**.

**Step 4**
Select **Cisco Prime LAN Management Solution 4.2**.

**Step 5**
Select the required feature specific update from the product tree.

**Step 6**
Select the required device package updates from the product software type.

**Step 7**
Select a product release version from the Latest Release folder.

The device packages corresponding to the selected product version display at the right of the web page.

**Step 8**
Locate the device package update files which you want to download.

**Step 9**
Click the **Download Now** button to download and save the device package file to any local directory on LMS Server.

See the Supported Devices Tables for LMS 4.2 for more information about supported devices:
