ılıılı cısco

Deployment Guide

Cisco Prime LAN Management Solution 4.1

Deployment Guide

September, 2011

Contents

Cisco Prime LMS 4.1	4
Introduction	4
About the Deployment Guide	4
Useful Web Resources	4
LMS Work Flow	4
Setting Up Devices on the Network	5
Device Configuration	6
Configuring Communication Protocols	/
SNMP Settings	/
System Reload	0
Secure Copy Protocol	9 Q
HTTP and HTTPS	10
Configuring Other Protocols.	10
Cisco Discovery Protocol	10
Syslog Messages	11
Protocol Setup on LMS Server	12
Configuration Management	12
Device Secondary Credentials	13
Software Image Management	14
Cisco Prime LMS Installation	14
Installation Checklist	14
Licensing Process	16
Steps to Follow for Licensing LMS	16
New Installation of LMS 4.1 on Windows	17
New Installation of LMS 4.1 Using Soft Appliance	19
Verifying the LMS 4.1 Installation	26
Ports Used by LMS Applications	27
Getting Started with Cisco Prime LMS 4.1	29
Data Migration	30
General System Settings	32
Multiserver Configuration	32
Other System Settings	34
RCP and SCP Credentials	34
Browser-Server Security Mode	35
Backup	35
Authentication Settings	36
Device Management	30
	30
User Management	40
User Roles	40
Adding Users	42
Software and Device Updates	45
Advanced Configurations	46
Monitoring	46
Fault Management Settings	46
Configuration Management	46
Inventory and Configuration Management	47
Business Scenario	47
Configuration Management Overview	47
Inventory Management Overview	48
Software Image Management	51
Configuration ArchiveManagement	52

Configuration Collection Transport Settings	
Config Editor	
NetConfig	54
Topology	
Template Center	
Monitoring	59
Monitoring Dashboard	
Customizing the Monitoring Dashboard Using Portlet	
Poller Configuration on an Existing Portlet	
Fault Management	61
Fault Monitor	61
Performance Monitoring	
Creating Thresholds and Notifications	63
IPSLA Monitoring	
Reports	69
Work Centers	72
Server Administration	72
Log Rotation.	
– s Database Backup	
Backing Up Using CLI	75
Restoring Data on Solaris and Linux	75
Restoring Data on Windows	76
Cisco Smart Interactions	77
Appendix A: List of Acronyms and Features	

Cisco Prime LMS 4.1

Introduction

Cisco Prime[™] LAN Management Solution (LMS) is an integrated suite of management functions that simplify the configuration, administration, monitoring, and troubleshooting of Cisco[®] networks. Built on the latest web 2.0 Internet-based standards, Cisco Prime LMS allows network operators to manage a borderless network through a browser-based interface that can be accessed anytime from anywhere within the network. Cisco Prime LMS 4.1 improves the overall user experience and continues to provide new workflows built on functional partitioning that aligns the product with the way network operators do their jobs. Once installed, prepackaged monitoring and troubleshooting dashboards provide actionable information to quickly isolate and fix network problems before they affect services.

Configuring and deploying updates to the network has never been easier with the Template Center, which now incorporates Cisco Smart Business Architecture (SBA) templates that are based upon Cisco Validated Designs, simplifying platform and technology rollout and reducing the chance for errors. Work Centers provide a single area where guided workflows give step-by-step instructions to help operators quickly provision, monitor, and manage new Cisco value-added technologies and solutions, such as medianet, EnergyWise, TrustSec/Identity, Auto Smartports, and Smart Install.

For detailed product information related to LMS, refer to the product portal at http://www.cisco.com/en/US/prod/netmgtsw/prime.html.

About the Deployment Guide

This deployment guide considers scenarios where all applications reside on a single server and provides tips and suggestions on configuring the server and getting the basic functions of applications running. Discussions related to multiserver deployment can be found in the LMS 4.0 Large Scale Deployment Guide, available at http://www.cisco.com/en/US/products/ps11200/prod_white_papers_list.html.

Tip: In short, the decision on whether to use single or multiple LMS servers to manage the network depends on:

- How many devices are managed by the LMS server. In LMS 4.1, one single server can manage up to 5000 devices.
- How the LMS applications are used. For example, fault management is used extensively to poll the devices.

Useful Web Resources

Product Bulletin: http://www.cisco.com/en/US/products/ps11200/index.html

Supported Device List (check out the Generic Device Support section in Chapter 7, Resource Manager Essentials[RME]):

http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/device_support/table/lms4 1sdt.html

Evaluation Copy (valid for 100 devices and 90 days; copies of both Windows and Solaris are available): <u>http://www.cisco.com/go/nmsevals</u>

Release Notes: http://www.cisco.com/en/US/products/ps11200/prod_release_notes_list.html

LMS Work Flow

The steps below summarize LMS setup workflow, which covers the whole lifecycle of LMS server from initial setup to ongoing operations. The following section illustrates in detail each of the steps mentioned in this workflow.

 The first step in the workflow is to turn on Cisco Discovery Protocol, Simple Network Management Protocol (SNMP), and other credentials such as Telnet username/password on the devices so that the devices can be discovered and managed by Cisco Prime LMS.

Tools used: Command-line interface (CLI) tools such as console connection, Telnet, Secure Shell (SSH) Protocol, and so on.

 Once LMS server is installed, LMS 4.1 guides you to do the initial setup through the Getting Started workflow from the Admin menu. See Figure 1. This includes configuring basic server settings, automatically discovering the devices, or manually adding devices.



Getting Started
✓Introduction
Getting Started with LMS New features in LMS 4.1
> Data Migration
> General System Settings
> Multiserver Configuration
> Other System Settings
> Device Management
>User Management
> Software and Device Updates
> Advanced Configurations

Setting Up Devices on the Network

Cisco Prime LMS 4.1 helps in managing Cisco devices on the network. Before LMS 4.1 can function properly, the network devices that LMS interfaces with must be set up correctly in order to communicate with the Cisco Prime LMS server. For example, the SNMP community strings must match between the device and the Cisco Prime LMS server. The information provided in this chapter is a general description of the means and procedures recommended to make sure that the network devices are set up properly.

Note: This chapter provides a great deal of information on the device configuration procedures required to manage devices using Cisco Prime LMS. Keep in mind that this document is not intended to be a comprehensive configuration guide for LMS 4.1. For additional LMS configuration details, please contact a Cisco certified network engineer (if possible) and refer to pertinent documents that are posted on Cisco.com.

Prior to LMS deployment, in the case of Cisco IOS[®]Software and Catalyst[®] Operating System devices, all configuration changes must be saved to nonvolatile memory (NVRAM) using the following command:

write memory

This command saves any pre-LMS deployment configuration changes. After LMS is deployed, configuration changes will be saved automatically where appropriate and no user intervention is required.

Also note that newer versions of Catalyst OS devices have separate running and startup configurations.

Device Configuration

This section describes the generic elements in the device configuration.

System Name

Each Cisco IOS device in the network must have a unique system name (sysname) in order to be managed. The system name is also populated in the Cisco Discovery Protocol table. If there are duplicate system names, LMS will discover only one device by that name on the network. On Cisco IOS devices, the domain name also affects the system name.

You can set up the system name using the following commands.

For Cisco IOS devices:

hostname<name>

For Cisco Catalyst OS devices:

set system name <name>

Domain Name

You can set a domain name on a Cisco IOS or Catalyst OS device. To set up the domain name, use the following commands.

For Cisco IOS devices:

ip domain-name <name>

For Cisco Catalyst OS devices:

set system name <name with domain name>

Command-Line Prompts

To utilize the NetConfig capability to execute batch changes on devices, Cisco device command-line prompts should meet the requirements described in this section.

Note: Customized prompts should also fulfill these requirements.

For Cisco IOS devices:

- Login prompt should end with an angle bracket (>).
 For example: Cisco>
- Enable prompt should end with a pound sign (#).

For example: Cisco#

For Cisco Catalyst OS devices:

• Enable prompt must end with (enable).

For example: Cisco (enable)

Configuring Communication Protocols

LMS uses various protocols to communicate with the devices. These protocols must be configured properly on both the LMS server and devices so that they can communicate to each other. See Table 1 for a list of device credentials for LMS applications.

Application	Telnet/SSH Password	Enable Password	SNMP Read Only	SNMP Read/Write
Common Services	Not required	Not required	Required	Required
Topology and Identity Services	Not required	Not required	Required	Required
Fault Monitoring	Not required	Not required	Required	Not required
IPSLA Monitoring	Not required	Not required	Required	Required
Performance Monitoring	Not required	Not required	Required	Not required
TrendWatch	Not required	Not Required	Required	Not Required
Inventory	Not required	Not required	Required	Not required
Configuration Management (Telnet)	Required	Required	Required	Not required
Configuration Management ¹ (TFTP) ²	Not required	Not required	Required	Required
NetConfig	Required	Required	Required	Required
Config Editor	Required	Required	Required	Required
NetShow	Required	Required	Required	Not required
Software Management	Required ³	Required ³	Required	Required
Port and Module Configuration	Required	Required	Required	Required
EnergyWise	Required	Required	Required	Required
Auto Smartports	Required	Required	Required	Required
Identity Services	Required	Required	Required	Required
Smart Install	Required	Required	Required	Required

Table 1. Applications and Device Credentials

SNMP Settings

LMS supports SNMPv1/v2c and SNMPv3 with both AuthNoPriv mode and AuthPriv. SNMPv3 AuthPriv is a new feature introduced since LMS 3.0.1.

SNMP settings include both the read-only community string and the rewritable (RW) community string. The readonly community string is used to perform "snmp get" operations on MIB objects to collect information such as inventory, interface utilization, and so on. The rewritable community string is used in various cases. For example, the RW string is used in LMS for:

- Configuration deployment
- Software image management

Cisco Prime LMS can collect device configurations by either SNMP-write, which triggers TFTP, or by grabbing output from a CLI "show running" command (requiring Telnet or SSH access to the device).

In image deployment the RW community string is used to trigger the TFTP connection and also for the system reboot after the image is downloaded. The RW string is also used in CiscoWorks Campus Manager for configuration changes such as fixing discrepancies.

¹ Configuration download also uses Trivial File Transport Protocol (TFTP). Hence, SNMP Read/Write credentials are required.

² The file vlan.dat can be fetched only if the Telnet password and Enable password are supplied.

³ Required in the case of a few devices such as PIX[®] devices, Cisco 2950 Series Switches.

For information on SNMP settings, refer to

http://www.cisco.com/en/US/customer/tech/tk648/tk362/technologies_tech_note09186a0080094aa4.shtml.

System Reload

After a software image distribution operation using LMS is completed, LMS will reload the device if specified in the image distribution job. LMS will be able to reload any device (Cisco IOS or Catalyst OS) only if an SNMP manager (in this case LMS) is allowed to reset the agent.

The following command is needed on Cisco IOS devices only:

snmp-server system-shutdown

Telnet/SSH

Telnet is one of the basic protocols that can be used by LMS for configuration management. You can enable Telnet using the following commands.

To enable Telnet on Cisco IOS devices and Catalyst OS devices, enter these commands:

```
line vty 0 4
password<password>
transport input telnet
```

Note: More than four vty lines can be selected for login.

Different authentication on different vty lines is not supported.

SSH provides for a secure communication with the device.

Cisco IOSSoftware

The following example configures SSH control parameters on a router running Cisco IOS Software:

```
Router> config terminal
Router (config) # hostname hostname <the name of the router>
Router (config) # ip domain-name domainname <a domain that the router services>
Router (config) # crypto key generate rsa
Router (config) # aaa new-model
Router (config) # username <username> password <password>
Router (config) # ip ssh time-out <seconds>
Router (config) # ip ssh authentication-retries <integer>
Router (config) # line vty 0 4
Router (config-line) # transport input SSH
```

Make sure to do this for all vty lines.

Catalyst OS

The following examples configure SSH in Catalyst OS:

```
(enable) set crypto key rsa 1024
(enable) set ip permit enable ssh
```

Remote Copy Protocol

Remote Copy Protocol (RCP) is one of the protocols that can be used by LMS for configuration management and software image management. For LMS to be able to provide configuration and software management using RCP, it must be enabled on the devices.

RCP can be enabled only on devices running Cisco IOS Software using the following sample commands:

```
username cwuser password 7 000C1C0A05
ip rcmd rcp-enable
ip rcmd remote-host cwuser 172.17.246.221 cwuser enable
ip rcmd remote-username cwuser
```

Note: The value of <remote-username> and <local-username> entered in the device should match the RCPUser value provided in the LMS server. The default value is cwuser. This value can be reset by traversing through the following user interface links in LMS server: Admin \rightarrow System \rightarrow System Preferences. See Figure 2.

Figure 2. Setting the RCP User Value

w / Edit System Preferences	
E mail Settings	
SMTP Server:	localhost
Administrator E-mail ID:	yourusername@example
Enable E-mail Attachment:	
Maximum Attachment Size:	2 MB 💌
Other Settings	
RCP User:	cwuser
SCP User:	
SCP Password:	
SCP Verify Password:	

Secure Copy Protocol

The Secure Copy Protocol (SCP) feature was introduced in Cisco IOS Software Release 12.2(2) T.

To enable and configure a Cisco router for SCP server-side functionality, perform the steps in Table 2.

	Command	Purpose
Step 1	Enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router (config)# aaa new-model	Sets authentication, authorization, and accounting (AAA) at login.

	Command	Purpose
Step 4	Router (config)# aaa authentication login default group tacacs+	Enables the AAA access control system. Complete syntax: aaa authentication login {default list-name} method1 [method2]
Step 5	Router (config)# aaa authorization exec default group tacacs+	Sets parameters that restrict user access to a network. The exec keyword runs authorization to determine if the user is allowed to run an EXEC shell; therefore, you must use it when you configure SCP. Syntax: aaa authorization {network exec commands level reverse-access configuration} {default list-name} [method1 [method2]]
Step 6	Router (config)# username superuser privilege 2 password 0 superpassword	Establishes a username-based authentication system. You may skip this step if a network-based authentication mechanism - such as TACACS+ or RADIUS - has been configured. Syntax: usernamename[privilegelevel] {passwordencryption-type encrypted-password}
Step 7	Router (config)# ip scp server enable	Enables SCP server-side functionality.

HTTP and HTTPS

The Cisco IOS HTTP server provides authentication, but not encryption, for client connections. The data that the client and server transmit to each other is not encrypted. This leaves communication between clients and servers vulnerable to interception and attack.

Use the following command to enable HTTP mode:

ip http server

The Secure HTTP (HTTPS) feature provides the capability to connect to the Cisco IOS HTTPS server securely. It uses Secure Sockets Layer (SSL)⁴ and Transport Layer Security (TLS) to provide device authentication and data encryption.

Configuring Other Protocols

Cisco Discovery Protocol

Cisco Common Services uses both Layer 2 (Cisco Discovery Protocol) and Layer 3 (Border Gateway Protocol [BGP], Open Shortest Path First [OSPF], Address Resolution Protocol [ARP], and routing tables) to discover devices. Cisco Discovery Protocol is the default protocol to discover Cisco devices on the network. Cisco Discovery Protocol is a Cisco proprietary Layer 2 protocol that is media and protocol independent and runs on all Cisco manufactured equipment. A Cisco device enabled with Cisco Discovery Protocol sends out periodic interface updates to a multicast address in order to make itself known to neighbors. Since it is a Layer 2 protocol, these packets (frames) are not routed.

Enabling Cisco Discovery Protocol on devices allows Common Services to learn information about neighboring devices and to send SNMP queries to those devices.

Enable/Disable Cisco Discovery Protocol on Cisco IOS devices:

Cisco Discovery Protocol is enabled on Cisco IOS devices by default. To manually enable the Cisco Discovery Protocol capability on Cisco IOS devices use the following commands:

- To enable Cisco Discovery Protocol globally:
 - cdp run

⁴ This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more details please visit <u>http://www.openssl.org/</u>.

To enable Cisco Discovery Protocol on specific interfaces only:

cdp enable

Use the no command to disable Cisco Discovery Protocol capability on Cisco IOS devices.

Enable/Disable Cisco Discovery Protocol on Cisco Catalyst OS devices:

Cisco Discovery Protocol is enabled on Cisco Catalyst OS devices by default. To enable Cisco Discovery Protocol capability manually on Catalyst OS devices use the following commands:

To enable Cisco Discovery Protocol globally:

set cdp enable

• To enable Cisco Discovery Protocol on specific ports only: set cdp enable [mod/port]

Use the set cdp disable command to disable Cisco Discovery Protocol on Catalyst OS devices.

Do not run Cisco Discovery Protocol on links that don't need to be discovered, for example, connection to the Internet and end host connection ports on access switches.

To protect from Cisco Discovery Protocol Denial of Service (DoS) attacks, do not enable Cisco Discovery Protocol on links that are connected to non-Cisco devices, and if the non-Cisco devices do not support Cisco Discovery Protocol, LMS 4.1 provides Link Layer Discovery Protocol (LLDP) as another protocol for discovery purposes. LLDP functions at Layer 2 and is supported by most other vendors. This release of LMS 4.1 will support only IPv4 for LLDP.

Note: Certain non-Cisco devices support Cisco Discovery Protocol. If you enable Cisco Discovery Protocol on the Cisco devices connected to non-Cisco devices, they will appear on the topology map and Cisco Discovery Protocol is a must for the topology map.

Syslog Messages

Syslog messages can be enabled on Cisco devices to use fully the capability of LMS. LMS has a built-in syslog receiver/analyzer, and it can invoke automated actions based on the content of the syslog message.

Please refer to

http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml# topic1

Another way to turn on syslog devices is to use the LMS NetConfig functionality. With NetConfig, users can create a job to deploy syslog configuration commands to multiple devices at the same time. NetConfig will be discussed later in this document (please refer to "Create a NetConfig Job to Enable Syslogs on Devices and Configure LMS Server as Receiver" in the "Netconfig" section), but Figure 3 shows an example of syslog configuration:

Figure 3. An Example Syslog Configuration

			Syslog C	Configura	tion				
Comm	on Paramet	ers							
Loggi	ng Host	_			_				
Action:	Add	•	Hosts (com	ima separat	ed): 1	0.10	1.10.1		
IOS Pa	arameters						_		
Loggi	ng On								
Action:	No Change	•							
Loggi	ng Facility								
Action:	No Change	•	Parameter:	auth	•				
Loggi	ng Level								
Buffer	ed								
Action:	No Change	•	Conditions:	Default		•			
Conso	ole								
Action:	No Change	•	Conditions:	Default		•			
Monite	or								
Action:	No Change	•	Conditions:	Default		•			
Trap									
Action:	No Change	•	Conditions:	Default		•			
						A	onlicable	Neuices	
							- Includio		
				(Sav		Reset	Canc	el

Protocol Setup on LMS Server

One of the most important areas of setup is LMS protocol setup. LMS uses various protocols for configuration and software management. Network administrators can assign the protocols to be used in LMS for configuration management and software management.

Configuration Management

You can set the protocols and order configuration management applications such as Archive Management, Config Editor, and NetConfig use to download configurations and to fetch configurations. The available protocols are Telnet, TFTP, RCP, SSH, SCP, and HTTPS.

To setup protocol ordering for configuration management, go to Admin→Network→Config Collection Settings→Config Transport Settings.

Figure 4. Configuring Transport Settings

t Settings		
Archive Mgmt 💌		
Available Protocols		Selected Protocol Order
TELNET TFTP SSH RCP HTTPS SCP	Add >> << Remove	TELNET TFTP SSH RCP HTTPS
Available Protocols TELNET TFTP SSH		Selected Protocol Order TELNET TFTP SSH
HTTPS RCP SCP	< Remove	HTTPS
	Archive Mgmt Archive Mgmt Available Protocols TELNET TFTP SSH RCP Available Protocols TELNET TFTP SSH HTTPS RCP SCH SCP SCP	Archive Mgmt Available Protocols TELNET TFTP SSH RCP Available Protocols Available Protocols TELNET TFTP SSH HTTPS RCP SCP Add >> << Remove <<< Remove <<< Remove

As in Figure 4 for the Config Fetch task, LMS will first use Telnet, and if Telnet to the device fails, LMS will fallback to the next protocol in the order listed, in this case TFTP. LMS 4.1 also allows you to change this protocol order. It is recommended to use SSH as a secure protocol between the server and the device.

Device Secondary Credentials

Once LMS discovers and adds all the network devices into its database, LMS uses the primary and secondary credentials to access these devices using the following protocols:

- Telnet
- SSH

The LMS server first uses the primary credentials to access the device. The primary credentials are tried out three times, and on failure the secondary credentials are tried out three times. Secondary credentials are used as a fallback mechanism for connecting to devices. See Figure 5.

For instance, if the AAA server is down, accessing devices using their primary credentials will lead to failure.

Figure 5.	To specify fallback to the secondary credentials,	select Admin →Collection Settings→config→Secondary
-	Credentials settings (see Figure 5) Secondary	Credentials

Secondary Credenti	als
Fallback to Seconda	ary Credentials
	Apply Cancel

Software Image Management

Similarly, software management attempts downloading the software images based on the protocol order specified. While downloading the images, software management uses the first protocol in the list. If the first protocol in the list fails, these jobs use the second protocol and so on, until software management finds a transport protocol for downloading the images. The supported protocols are RCP, TFTP, SCP, and HTTP.

Using Admin-Network-Software Image Management-View/Edit Preferences, you can define the protocol order that software management has to use for software image downloads. Use the Add and Remove buttons for selecting the protocol order. See Figure 6.

Figure 6. Defining the Protocol Order for Software Image Downloads

Repository						
Image Location *: /var/	adm/CSCOpx/files	/rme/reposit	ory/			
Distribution						
Script Location					Provero	Clear
	00		wede		DIDWSe	Cibai
Script Timeout	50	Sect	inus			
	Available Protoc	cols	-	Selected I	Protocol Order	_
Image Transfer Protocol Order	RCP TFTP SCP HTTP		Add >>	SCP HTTP		
Use SSH for software image	upgrade and soft	tware image i	mport through CLI(wil	h fallback to T	ELNET).	
Recommendation						
Include Cisco.com images f	or image recomme	endation.				
Include General deploymen	t images.					
Include latest maintenance	release (of each	major release).			
V Include images higher than	running image.					
Include same image reature	e subset as runnir	ig image.				
Password Policy						
Enable Job-based Password						

Cisco Prime LMS Installation

Cisco Prime LMS 4.1 can be installedon the Windows or Solaris operating system or as a soft appliance. A soft appliance comes as an Open Virtual Archive (OVA) file, which is an open virtualized format to deploy the software package directly to your virtual machine (VM) systems. The OVA file comes with an embedded Red Hat Linux operating system with database and application.

Installation Checklist

Before you install LMS 4.1, make sure that:

- The server and client systems have the recommended hardware and software requirements. Please refer to the installation guide at <u>http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/install/guide/prereq.</u> <u>html#wp1109415</u>
- You have closed all open or active programs. Do not run other programs during the installation process.
- You have disabled Terminal Services on the Windows operating system in the Application mode. If you have enabled Terminal Server in Application mode, disable the Terminal Server, reboot the system, and start the installation again. However, you can enable Terminal Services in the Administration mode.

- If you have configured Remote Syslog Collector (RSC) on a different server, you must upgrade RSC to RSC 5.1. See **Installing the Remote Syslog Collector** for further information.
- You have disabled the virus scanner on your system during installation.
- You have configured the recommended swap space. Refer to
 <u>http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/install/guide/prereq.
 html#wp1109415</u>.

For Windows and Solaris, after you uninstall earlier versions of LMS like LMS 3.2, you haveremoved the LMS logo manually if it is not removed during installation. For supported migration path, please refer to http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/install/guide/instl.ht ml#wp1581295.

- Make sure to set up the High Availability (HA) and Disaster Recovery (DR) environment before installing LMS By default, SSL is not enabled on the Cisco Prime server.
- While launching Cisco Prime, network inconsistencies might cause installation errors if you are installing from a remote mount point.
- You disable any popup blocker utility that is installed on your client system.
- LMS 4.1 is installed in the default directories:
 - On Solaris and soft appliance: /opt/CSCOpx
 - On Windows, 64 bit: SystemDrive:\Program Files<x86>\CSCOpx
 - On Windows, 32 bit: SystemDrive:\Program Files\CSCOpx
 - Where SystemDrive is the Windows operating system installed directory.
- If you selected another directory during installation, the application is installed in that directory.
- The destination folder does not contain the following special characters:
 - On Solaris and soft appliance:

```
! @ # $ % ^ & * ( ) + | } { " : [ ]; ' ? <>, . ` = ~
```

On Windows:

! @ # \$ % ^ & * () + | } { " []; '/? <>, .`=

• If errors occured during installation, you have checked the installation log file:

On Solaris and soft appliance, check the installation log file

/var/tmp/Cisco_Prime_install_YYYYMMDD_hhmmss.log for LMS 4.1 installation

Where **YYYYMMDD** denotes the year, month and date of installation and **hhmmss** denotes the hours, minutes and seconds of installation.

For example:

/var/tmp/Cisco Prime install 20110721 182205.log

On Windows, check the installation log in the root directory on the drive where the operating system is installed. Each installation creates a new log file.

For example, for LMS 4.1, the installation log file is:

C:\Cisco_Prime_install_YYYYMMDD_hhmmss.log, where YYYYMMDD denotes the year, month and date of installation and hhmmss denotes the hours, minutes and seconds of installation.

For example:

```
C:\Cisco_Prime_install_20100721_182205.log
```

- You have disabled HP OpenView in order to run a faster installation. If HP OpenView is running on your system, installation will take more time.
- You have installed the latest Device Package updates to help ensure that you have the latest device support and bug fixes for LAN Management Solution.
- You have enabled Domain Name System (DNS) on the server so the device names can be resolved against IP addresses. If DNS is not present, create a local hosts file to help resolve the device names.
- You have registered the product and received a permanent license (recommended by Cisco).

You can press **Ctrl-C** (on Solaris, and not on soft appliance) or click **Cancel** (on Windows) at any time to end the installation. However, any changes to your system will not be undone.

For example, if any new files were installed or if they were any changes to the system files, you need to manually clean up the installation directories.

Note: We recommend that you do not terminate the installation while it is running.

Licensing Process

The Cisco Prime LMS product provides features such as software-based product registration and license key activation technologies. Product Authorization Key (PAK) ID refers to the identification key that you must enter while registering your product in Cisco.com to receive the product serial license key.The PAK is normally printed on the software claim certificate that is part of the product DVD kit.With the new ordering options introduced you can receive the digital PAK IDs through online delivery as well.

For additional information on licensing, please refer to

http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/install/guide/prep.html#wp 1327286.

Steps to Follow for Licensing LMS

To license Cisco Prime LAN Management Solution, follow the steps below as shown in figure 7:

Figure 7. Steps in the licensing process



Step 1. Log onto Cisco.com to get your license file. If you are a registered user of Cisco.com, get your license from http://www.cisco.com/go/license.

If you are not a user of Cisco.com, get your Cisco.com user ID from <u>http://tools.cisco.com/RPF/register/register.do</u>. Once you get your Cisco.com user ID, log on to

http://www.cisco.com/go/license to get your license file.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- Step 2. Register the LMS product with Cisco.com using the PAK to get your license file.
- Step 3. Install the license file:

If you have obtained the LMS license before installation:

- a. Select the first LMS application you wish to install (ideally Common Services 3.1), and when prompted:
 - On Windows, select the first option button and click **Browse** and use the File browse window to locate the license file directory.
 - On Solaris, select L for License File after you accept the licensing agreement and continue installing the application.
- b. Click **Next** to install the license file.

If you want to convert an evaluation copy to a licensed copy:

- After you install LMS 4.1, copy this license file to the Common Services server into a directory with read permissions for the user name **causer** in the user group **causers**.
- Select Admin→System→License management.

The License Administration page appears.

• Click Update.

A file browser appears.

• Enter the path to the new license file in the License File field and click OK.

The system verifies whether the license file is valid and updates the license.

Note: The license file obtained is platform independent and thus can be used in both Windows as well as Solaris operating systems.

New Installation of LMS 4.1 on Windows

Thanks to the single-package installation design, the LMS installation programs on both Windows and Solaris are user friendly and fail-proof. Figure 8 provides a flow diagram for Windows installation.



Figure 8. A Flow Diagram for Windows Installation of Cisco Prime LMS

New Installation of LMS 4.1 on Solaris.

Figure 9 provides a flow diagram for Solaris installation.



Figure 9. A Flow Diagram for Windows Installation of Cisco Prime LMS

New Installation of LMS 4.1 Using Soft Appliance

You can install the LMS soft appliance using the LMS 4.1 OVA image from the LMS 4.1 DVD.

- Make surethat your system meets the recommended hardware and software specifications specified in the server requirements section for Solaris.
- It takes approximately 30 minutes (deployment in the local system) and 50 minutes (deployment in the network) to install the soft appliance on a virtualized environment.
- Soft appliance OVA software can be installed only in the VMware environment.

Note: You need not install any soft appliance image on the VM before installing LMS 4.1, as the LMS 4.1 OVA image has an embedded RedHat Enterprise soft appliance.

Follow the steps below to install the LMS 4.1 soft appliance image (OVA):

- Step 1. Invoke the VMware vSphere client.
- **Step 2.** Enter the IP address or name of the host that needs to be directly managed. To manage multiple hosts, enter the IP address or name of a vCenter server.
- Step 3. Enter the username and password of the VMware server.
- Step 4. Click Login.
- **Step 5.** Select **File → Deploy OVF Template**. See Figure 10.
- Figure 10. The Deploy OVF Template Window



- Step 6. Click Browse to select the source Open Virtualization Format (OVF) template from your local file system or enter a URL to download the OVF package from the Internet.
- Step 7. Click Next. The Deploy OVF Template OVF Template Details window appears (Figure 11). You can verify the OVF template details.

Home 🕹 🚮 In	ventory) 🛐 Inventory			
10.77.163.130 CS-DEV-131 CS-DEV-132	CS-DEV-131 Deploy OVF Template OVF Template Details Verify OVF template details			
	Surce OVF Template Details Name and Location Detastore Deta Format Ready to Complete	Product: Version: Vendor: Publisher: Download size: Size on disk: Description:	Cisco_Prime_LMS_4_1 No certificate present 4.8 GB 7.4 GB (thin provisioned) 360.0 GB (thick provisioned) Cisco_Prime_LMS_4_1	
ecent Tasks	Help		< Back Next > Car Name, Target or St.	ncel

Figure 11. The Deploy OVF Template - OVF Template Details Window

Step 8. Click Next.

The Deploy OVF Template -Name and Location window appears (Figure 12).



Figure 12. The Deploy OVF Template - Name and Location Window

Step 9. Enter the name of the deployed template.

Note: Ensure that you provide a unique template name that does not exceed 80 characters. The unique template name refers to the virtual host deployed in the ESX/ESXi server.

Step 10. Click Next.

The Deploy OVF Template -Datastore window appears (Figure 13).

Edit View Inventory Adn	inistration Plug-ins Help Inventory () (1) Inventory							
10.77.163.130	CS-DEV-131							
CS-DEV-132	📕 🛃 Deploy OVF Template							
	Datastore Where do you want to	store the virtual machine f	lles? which to store th	e VM files:				
	OVF Template Details	L News	Canada a	Devidenced	Free	Trees	This Devidelenter	1.4.4.4.4
	Name and Location	[datactore1]	Lapacity	FTOVISIONED	1 26 TP	UMES	Furported	Single
	Datastore	[datastore1]	1.30 IB	5/7.00 MB	1.36 IB	VMES	Supported	Single
		¢		0		. 1[2

Figure 13. The Deploy OVF Template - Datastore Window

Step 11. Select a datastore where you want to store the virtual machine files.

Step 12. Click Next.

The Deploy OVF Template -Disk Format window appears (Figure 14).

Figure 14. The Deploy OVF Template - Disk Format Window



Step 13. You can select either Thin provisioned format or Thick provisioned format.

Note: We recommend that you choose Thick provisioned format. If you use Thick provisioned format, you must make sure that your system meets the recommended hardware and software requirement specified in the server requirements section for Solaris.

Step 14. Click Next.

The Deploy OVF Template -Ready to Complete window appears (Figure 15). This window displays the deployment setting details.

Figure 15. The Deploy OVF Template - Ready to Complete Window



Step 15. Click Finish to start the deployment task.

Note: The deployment task takes approximately 50 minutes to complete.

- Step 16. Select a server thathas the deployed template name specified in Step 9 from the servers listed on the left pane of the vSphere client window.Right-click the selected server and select Power → Power On to start the server.
- Step 17. Select the Console tab.

The Welcome screen appears.

Step 18. Press Enter in the console window to continue with the next step.

Step 19. Enter the following configuration details of the server:

- Hostname (should not exceed 19 characters)
- IP Address
- IP Netmask

- Default Gateway
- DNS Domain Name
- Primary Name Server
- Secondary Name Server (optional)
- Primary NTP Server
- Secondary NTP Server (optional)
- System Time Zone

Type **h** to see the list of supported time zones, and enter the time zone value. For example, Brazil/DeNoronha. You can check **Supported Server Time Zones and Offset Settings** for the list of values supported.

• Username

Enter the username to access the LMS appliance console. This user will have the privilege to enable the shell access. The default username is sysadmin. You cannot use root as the username as it is a reserved username. You can use only alphanumeric characters for the username.

Password

Enter the sysadmin password. By default, this password will be set as the shell password.

Confirm Password

Enter the sysadmin password for confirmation.

Admin Password

Enter the password for the admin account to log into LMS using the browser. This password must contain a minimum of five characters and will also be used for the System Identity account.

Confirm Password

You can enter the admin password for confirmation.

Step 20. The following message appears:

For security reasons, passwords are not displayed. Do you want to view all the passwords? (Y/N) [N]:

Step 21. If you enter Y, the following passwords will be displayed.

- · Admin user account password
- System identity user account password
- System-generated database password

The default option is N.

Step 22. It will take 15 to 20 minutes to process the databaseengine.

Step 23. The server is automatically rebooted.

Note: If you want to power off the VM server from the ESX server, you must do so only after stopping the daemons. You must not power off the VM while the daemons are running.

This completes the soft appliance installation. If you would like to change any server settings, please refer to http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/install/guide/instl.html#wp1639616.

Verifying the LMS 4.1 Installation

After you install Cisco Prime LMS 4.1 on Windows, you must verify the installation. To do this:

Launch Cisco Prime LMS: <u>http://server_name:1741</u>

where server_name is the name of the Cisco Prime LMS server and 1741 is the TCP port used by the server.

In normal mode (HTTP), the default TCP port for Cisco Prime LMS is 1741. When SSL (HHTPS) is enabled, the default TCP portis 443.

You can change the HTTPS port number of the Cisco Prime LMS server during the installation.

• Select Admin->System->Software Center->Software Update.

The Software Updates window (Figure 16) appears.

Figure 16. The Software Updates window

indles Installed		
		Showing 1-1 of 1 reco
Bundle Name 4	Version	Installed Date
1.LMS	4.1	20 Jun 2011
Rows per page: 100 💌		KCGo to page: 1 of 1 pages Go
oducte Installed		
oducts Installed	Version With Patch Level	Showing 1-1 of 1 reco
oducts Installed Product Name 4 . E LAN Management Solution	Version With Patch Level 4.1.0	Showing 1-1 of 1 rect Installed Date 20 Jun 2011, 20:49:41 UTC
oducts Installed Product Name 4 1. AN Management Solution Rows per page: 100	Version With Patch Level 4.1.0	Showing 1-1 of 1 reco Installed Date 20 Jun 2011, 20:49:41 UTC ICC to page: 1 of 1 pages Go

or

• Select Admin→System→Server Monitoring→Processes to see various process statuses (Figure 17).

show	only:	All						
		ProcessName 4	ProcessState	ProcessId	ProcessRC	ProcessSigNo	ProcessStartTime	Showing 69 reco
1.		1040	Never started	0	0	0	N/A	Not applicable
2,		AdapterServer	Program started - No mgt msgs received	4203	0	0	07/15/11 14:02:42	Not applicable
з.		AdapterServer1	Program started - No mgt msgs received	4204	0	0	07/15/11 14:02:42	Not applicable
4.		ANIDbEngine	Program started - No mgt msgs received	3276	0	0	07/15/11 14:02:05	Not applicable
5.		ANIServer	Running with busy flag set	5701	0	0	07/15/11 14:07:04	Not applicable
6.		ChangeAudit	Program started - No mgt msgs received	6413	0	0	07/15/11 14:07:28	Not applicable
7.		CmfDbEngine	Program started - No mgt msgs received	5271	0	0	07/15/11 14:06:37	Not applicable
8.		CmfDbMonitor	Running normally	5305	0	0	07/15/11 14:06:41	Not applicable
9.		CMFOGSServer	Program started - No mgt msgs received	5365	0	0	07/15/11 14:06:48	Not applicable
10.		ConfigMgmtServer	Running normally	6098	0	0	07/15/11 14:07:15	Not applicable
11. ∢		ConfigUtilityService	Running normally	6107	0	0	07/15/11 14:07:15	Not applicable

Figure 17. The Status of Various Processes

Ports Used by LMS Applications

Make sure the ports listed in Table 3 are open on the Cisco Prime LMS server, or are not used by other applications.

Table 3.	LMS Application Port	Usage

Protocol	Port Number	Service Name	Applications	Direction (of Establishment) of Connection
ТСР	49	TACACS+ and Access Control Server (ACS)	Common Services, Configuration and Software Image Management, Topology and Identity Services, Fault Management, IPSLA Monitoring	Server to ACS
ТСР	25	Simple Mail Transfer Protocol (SMTP)	CiscoWorks Common Services (PSU), Inventory, Configuration and Image Management	Server to SMTP server
ТСР	22	SSH	Common Services, Topology and Identity Services, Inventory, Configuration and Image Management	Server to device
ТСР	23	Telnet	Common Services, Topology and Identity Services, Inventory, Configuration and Image Management	Server to device
User Datagram Protocol (UDP)	69	TFTP	Common Services, Inventory, Configuration and Image Management	Server to device Device to server
UDP	161	SNMP	Common Services, CiscoView, Inventory, Configuration and Image Management, Topology and Identity Services, Fault Management, IPSLA Performance Management, and Device Performance Management	Server to device Device to server
тср	514	Remote Copy Protocol	Common Services	Server to device

Protocol	Port Number	Service Name	Applications	Direction (of Establishment) of Connection
UDP	162	SNMP traps (standard port)	Topology and Identity Services and Fault Management	Device to server
UDP	514	Syslog	Common Services, Inventory, Configuration and Image Management	Device to server
UDP	1431	Trap listener to MAC notification traps	Topology and Identity Services	Device to server
UDP	9000	Trap receiving (if port 162 is occupied)	Fault Management	Device to Server
UDP	16236	UT host acquisition	Topology and Identity Services	End host to Server
ТСР	443	CiscoWorks HTTP server in SSL mode	CiscoWorks Common Services	Client to server Server internal
ТСР	1741	CiscoWorks HTTP Protocol	CiscoWorks Common Services, CiscoView, Topology and Identity Services, Inventory, Configuration and Image Management, Fault Management, and Internetwork Performance Monitor (IPM	Client to server
UDP	42342	OSAGENT	Common Services	Client to server (for ANIServer)
ТСР	42352	ESS HTTP (alternate port is 44352/tcp)	Common Services	Client to server
ТСР	8898	Log server	Fault Management	Server internal
ТСР	9002	DynamID authentication (Device Fault Manager [DFM] broker)	Fault Management	Server internal
ТСР	9007	Tomcat shutdown	Common Services	Server internal
ТСР	9009	Ajp13 connector used by Tomcat	Common Services	Server internal
UDP	9020	Trap receiving	Fault Management	Server internal
UDP	14004	Lock port for ANIServer singlet on check	Topology and Identity Services	Server internal
ТСР	15000	Log server	Fault Management	Server internal
ТСР	40050- 40070	CSTM ports used by CS applications, such as OGS, DCR	Common Services	Server internal
ТСР	40401	LicenseServer	Common Services	Server internal
ТСР	43242	ANIServer	Topology and Identity Services	Server internal
ТСР	42340	CiscoWorks Daemon Manager - Tool for Server Processes	Common Services	Server internal
ТСР	42344	ANI HTTP server	Common Services	Server internal
UDP	42350	Event Services Software (ESS) (alternate port is 44350/udp)	Common Services	Server internal
ТСР	42351	Event Services Software (ESS) listening (alternate port is 44351/tcp)	Common Services	Server internal
ТСР	42353	ESS routing (alternate port is 44352/tcp)	Common Services	Server internal
ТСР	43441	Common Services database	Common Services	Server internal
ТСР	43455	Inventory, Configuration and Image Management Database	Inventory, Configuration and Image Management	Server internal
ТСР	43443	ANIDbEngine	Topology and Identity Services	Server internal
ТСР	43445	Fault history database	Fault Management	Server internal
TCP	43446	Inventory service database	Fault Management	Server internal

Protocol	Port Number	Service Name	Applications	Direction (of Establishment) of Connection
ТСР	43447	Event Promulgation Module database	Fault Management	Server internal
ТСР	44400- 44420	CSTM ports	Fault Management, Device Performance Management	Server internal
ТСР	47000- 47040	CSTM ports	Inventory, Configuration and Image Management	Server internal
ТСР	49154	UPMDbEngine	Device Performance Management	Server internal
ТСР	49155	OpsxmlDbEngine, JDBC/ODBC	CiscoWorks Assistant	Server internal
ТСР	49157	IPSLA Performance Management Database	IPSLA Management	Server internal
ТСР	50001	SOAPMonitor	Inventory, Configuration and Image Management	Server internal
ТСР	55000- 55020	CSTM ports for Topology and Identity Services	Topology and Identity Services	Server internal

Getting Started with Cisco Prime LMS 4.1

The LMS Getting Started workflow assists you in performing the tasks required to get your Cisco Prime LMS ready and to manage your Cisco networks.

When you login to Cisco Prime LMS server for the first time, the Introduction page of the Getting Started workflow appears. The Introduction page lists the new features added in Cisco Prime LMS 4.1. You can do the following tasks using the Getting Started workflow:

- Configuring email, cisco.com, and proxy settings
- Updating software and device packages
- Migrating data
- · Configuring RCP and SCP credentials, security, backup, and authentication settings
- Managing devices and credentials
- Managing user roles and users
- Linking to advanced functionalities and settings

You can configure these tasks stepbystep using the Getting Started workflow. You can also execute these tasks independently by selecting the task from the Getting Started assistant pane (Figure 18).

Figure 18. Getting Started Wizard

cisco Prime Cisco LAN Management Sol		admin Log Out About Feedback Help 💽 = 10 ->
My Menu + Monitor + Invent	ary + Configuration + Reports + Admin + Work Centers +	1 H
Admin > Getting Started		98 34 2911, 13+40 UTC
Getting Started with LMS		Getting Started
CiscoWorks LAN Management Solut	on (LMS) provides you with powerful features that enable you to configure, monitor, troubleshoot, and administer Cisco networks. CiscoWorks Getting	✓Introduction
Started helps you in setting up LMS a	nd in getting it ready to manage your network intrastructure.	Getting Started with LMS Newfeatures in LMS 4.1
P Improved Usability	🍯 EnergyWise	> Data Migration
		> General System Settings
e identity	Big Monitoring	> Multiserver Configuration
📕 Auto Smartports	😳 Smart Install	> Other System Settings
		> Device Management
E Report Center	Enhanced Troubleshooting Workflows	> User Management
💥 Template Center	1 Local CiscoWorks Authorization Mode	Software and Device Updates
		> Advanced Configurations
Do not show Getting Started wizar	d at next login	
Proceed to Data Migration		
Skip the rest of the workflow and proc	eed to Device Status dashboard	

You can follow the workflow by clicking the Proceed to Data Migration linkor, if you know the next step, you can click any of the steps on the right side under the Getting Started wizard.

Figure 19. Getting Started - Data Migration

My Menu • Monitor • Inver	ntory • Configuration • Reports • Admin • Work Centers •	Ťŵ
Admin > Getting Started		00 Jul 2011, 13:40 U
Getting Started with LMS		Getting Started
CiscoWorks LAN Management Sole	ution (LMS) provides you with powerful features that enable you to configure, monitor, troubleshoot, and administer Cisco networks. CiscoWorks Getting	~Introduction
Started helps you in setting up LMS New Features in LMS 4.1	in gelling it ready to manage your network infrastructure.	Getting Started with LMS New features in LMS 4.1
P Improved Usability	🍠 EnergWise	> Data Migration
		> General System Settings
E Identity	國語 Monitoring	> Multiserver Configuration
🛃 Auto Smartports	😨 Smart Install	> Other System Settings
		> Device Management
E Report Center	# Enhanced Troubleshooting Workflows	>User Management
💥 Template Center	25 Local CiscoWorks Authorization Mode	> Software and Device Updates
		> Advanced Configurations
Do not show Getting Started wize	ard at next login	
Proceed to Data Migration Skip the rest of the workflow and pro	xced to Device Status dashboard	

Data Migration

This section describes how you can perform data migration from the previous version of LMS to LMS 4.1. It is assumed that you have backed up your current LMS installation.

Important: You have to freshly install LMS 4.1on a new server and then perform data migration from the previous version of LMS thatwas backed up. The migration path is available for the following versions of LMS for Solaris and Windows

- LMS 4.0.1
- LMS 4.0
- LMS 3.2
- LMS 3.1
- LMS 3.0 December 2007 update
- LMS 2.6

For more information on data migration, please refer to

http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/install/guide/instl.html#wp1 581295.

To start data migration:

- 1. Store the backup archive on the server to which you want to migrate the data.
- 2. Go to the command prompt and stop the daemons using the following command:
 - For Windows:

net stop crmdmgtd

- For Solaris: /etc/init.d/dmgtd stop
- 3. Run the command:
 - For Windows:

NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl -d backup_directory

• For Solaris:

```
/opt/CSCOpx/bin/perl /opt/CSCOpx/bin/restorebackup.pl -d backup_directory
where NMSROOT is the Cisco Prime installation directory and backup_directory is the directory in which
the backup archive is located.
```

- 4. Once the migration is complete, start the daemons using the following command:
 - · For Windows:

net start crmdmgtd

• For Solaris:

/etc/init.d/dmgtd start

LMS 4.1 also supports data migration from Solaris to soft appliance if the customer has installed LMS 4.1 soft appliance in his network. The migration path is available from the following previous version of LMS (assuming LMS 4.1 soft appliance is already deployed into another VM):

- LMS 4.0.1
- LMS 4.0
- LMS 3.2

To start data migration:

- 1. Store the backup archive on the server to which you want to migrate the data.
- 2. Stop the daemon manager by entering:
 - /etc/init.d/dmgtd stop
- 3. Restore the backed up data by entering:
 - NMSROOT/bin/perl NMSROOT/bin/restorebackup.pl -d BKP [-t temporary_directory]

where BKP is the backup directory.

You must enter the absolute path for **BKP**. For example, if **BKP** is under /opt, give the path as **NMSROOT/bin/perl NMSROOT/bin/restorebackup.pl** -d **/opt/BKP**.

- 4. Start the daemon manager by entering:
 - /etc/init.d/dmgtd start

For more information on data migration, please refer:

http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/install/guide/dmg.html#wp 1214701

Click the Proceed to General System Settings link for the next steps.

General System Settings

General system settings (Figure 19) allow administrators to configure email for LMS to send notifications in case of alerts and Cisco.com credentials to run end-of-sale, end-of-life, and Product Security Incident Response Team (PSIRT) reports as well as for the software image distribution feature.

Figure 20. The General System Settings Window

indicates requi	h	
mail Setting		
	SMTP Server* Incahost	
	Administrator E-mail ID * yourusername@example.com	
	Enable E-mail Attachment 🗹	
	Max. Size Of Attachment 2 MB *	
sco.com Cre	als	
sco.com Cre	als Usemame torn Password	
sco.com Cre	rats	
isco.com Cre	als	Apply

Multiserver Configuration

Multiserver configuration can be accomplished by selecting **Getting Started** \rightarrow **Multiserver Configuration** (see Figure 20).

Figure 21.	The Multiserver Configuration Window
------------	--------------------------------------

Hostname or IP Address	Server Display Name	Protocol	Port	DCR Mode	SSO Mode
Ims-41-eft	Ims-41-eft	http	1741	Standalone	Master
o convert server as Master or as Stan	dalone				
1. Change Device Credential Repo	ository Mode				
2. Change Single Sign-On Mode					
o convert server as Slave					
1. Prerequisite: Configure a master s	server. Hostname of the master server should b	e DNS resolvable.			
2. Configure Peer Server Certificat	te on master and slave.				
3. Configure System Identity Set	up on master and slave. Ensure system identity	vusername and password ar	e the same acro	ss all servers.	
4. Change Device Credential Repo	ository Mode to Slave				
5. Change Single Sign-On Mode t	o Slave				

The most common installations are stand-alone singleserver. If you are doing a multiserver deployment, then you can skip this section and click **Proceed to Other System Settings**.

Designate This Server as Master

• Change the Device Credential Repository (DCR) mode to Master.

By doing this, you are designating this server as master and informing LMS that the DCR is going to be updated and maintained on this master server. Choose **Master** as the DCR mode and click **Apply** (Figure 21).

Figure 22. Changing the DCR Mode to Master

DCR	Mode	
0	Standalone	
۲	Master	
0	Slave	
	Master:	
	SSL(HTTPS) Port of Master:	443
		Inform current slave of new Master Hostname
		Add new devices to Master. (Duplicate devices will not be added)
		Apply Cancel Help

- Change the SingleSign-On mode (Figure 22)
- Choose Master and click Apply

rigule zo. Change the Single Sign-On-	Single Sign-On Setup
---------------------------------------	----------------------

Single Sign-On Setup

Single Sign-On Setu	ab
🔘 Standalone (Norma	al)
Master (SSO Authority)	entication Server)
💿 Slave (SSO Regula	r Server)
Master Server N	ame: Ims-41-eft
(SSL) Port:	443
	Apply Cancel

Similarly, you can use the steps highlighted in Figure 23to designate a server or servers as slave instead of master.

Figure 24. Multiserver Configuration Options

Hostname or IP Address	Server Display Name	Protocol	Port	DCR Mode	SSO Mode
Ims-41-eft	Ims-41-eft	http	1741	Standalone	Master
o convert server as Master or as Star	ndalone				
1. Change Device Credential Rep	ository Mode				
2. Change Single Sign-On Mode					
o convert server as Slave					
	course Unstrained of the master course should be	ne DNS resolvable			
1. Prerequisite: Configure a master	server, musuriarrie ur une master server sribuiu p				
1. Prerequisite: Configure a master 2. Configure Peer Server Certifica	te on master and slave.	5 DIVS 10301000.			
1. Prerequisite: Configure a master 2. Configure Peer Server Certifica 3. Configure System Identity Set	ite on master and slave. Sup on master and slave.	y username and password a	re the same acro	ss all servers.	
Prerequisite: Configure a master Configure Peer Server Certifica Configure System Identity Set Configure System Identity Set Change Device Credential Rep	server, mostraine of the master server should to ite on master and slave. up on master and slave. Ensure system identity ository Mode to Slave	y username and password a	re the same acro	ss all servers.	
Prerequisite: Configure a master Configure Peer Server Certifica Configure System Identity Set Change Device Credential Rep S. Change Single Sign-On Mode	server, must have on the inacter server should be ite on master and slave. Ensure system identity on master and slave. Ensure system identity ository Mode to Slave to Slave	y username and password a	re the same acro	ss all servers.	

Click the Proceed to Other System Settings link to continue.

Other System Settings

In this section you can set up the following:

- · RCP and SCP credentials for the LMS server when LMS uses these protocols
- Browser-server security mode
- Backup LMS backup directory location and schedule
- Authentication settings You can choose from a number of authentication modes.

RCP and SCP Credentials

Use the System Settings window (Figure 24) to change the RCP and SCP credentials.

Figure 25. The System Settings Window

Admin > Getting Started			
System Settings			
RCP and SCP Credentia	ls		
You can change RCP and	d SCP credentials here		
RCP User	cwuser		
SCP User			
SCP Password			
SCP Verify Password			
			Apply
Browser-Server Security	Mode		
Backup			
Authentication Settings			

RCP User: Name used by a network device when it connects to Cisco Prime LMS server to run RCP. The user account must exist on UNIX systems and should also be configured on devices as local user in the IP rcmd configuration command. The default RCP username is cwuser.

SCP User: Name used by a network device when it connects to the Cisco Prime LMS server to run SCP. The username you have entered here is used for authorization while transferring software images using SCP. You must specify a username that has SSH authorization on a Solaris system. SCP uses this authorization for transferring software images.

SCP Password: Enter the password for the SCP user in this field. The password you have entered here is used for authentication while transferring software images using SCP. You must specify a username that has SSH authentication on a Solaris system. SCP uses this authentication for transferring software images.

SCP Verify Password: Reenter the SCP password in this field.

Click Apply.

Browser-Server Security Mode

Choose the HTTPS setting, either to enable or disable HTTPS (Figure 25).

Figure 26. Enable or Disable HTTPS in the System Settings Window

_		_
	Admin » Getting Started	_
	System Settings	
	RCP and SCP Credentials	
	Browser-Server Security Mode	
	You can change the security mode for browser-server communication	
	Current HTTPS setting: Disabled	
	Change HTTPS setting: O Enable HTTPS	
	Apply	
	Backup	
	Authentication Settings	

Backup

Specify the location of the backup directory in the Backup Directory field and the maximum number of backups to be stored in the Generations field.

In the Scheduler section, you can set the frequency of the backups by choosing Daily, Weekly, and so on. See Figure 27.

Admin > Setting Started		
System Settings		
DOD and COD Overdantials		
Browser-Server Security Mode		
Backup		
Backup Settings Backup Directory* /opt/C Generations* 0 Server date and time (when Scheduler	SCOpv/ms_backup Browse (0 turns of generations) the page was loaded) 09 Jul 2011, 15:00 UTC	
Dally Weekly Monthly	E-mail Start Time 00 * 00 * (HH.MM)	
		Apply
Authentication Settings		

Figure 27. Specify the Backup Directory and Schedule Backups in the System Settings Backup Window

Authentication Settings

Cisco Prime LMS provides various ways to authenticate a user. Administrator can choose from the optionsshown in Figure 27.

	Figure 28.	Options for Authenticating L	Jsers
--	------------	------------------------------	-------

P and SCP Credentials		
owser-Server Security Mode		
ckup		
uthentication Settings		
urrent authentication module is MS Active Direct	ory	
o change the authentication settings, select a mo	dule from the list given here and click Change	
 CiscoWorks Local 	 IBM SecureWay Directory 	
O KerberosLogin	C Local UNIX System	
MS Active Directory	Netscape Directory	
O RADIUS	○ TACACS+	
		Chang

Device Management

In this section there are two primary tasks:device management functions and device addition into LMS.

Device Management Functions

The check boxes determine which of the functions will be performed by LMS on the added devices. By default all the functions are checked. Unchecking any function will result in the lack of chosen functionality for the added devices. This is done to save LMS resources, but it is common to choose all the available functions.

Click the Proceed to Device Allocation Settings and then click on Device Addition link.
Figure 29. Device Addition

Device Allocation Settings
Devices can be auto allocated to the selected device management functions, or they can be allocated based on policies that can be configured. Allocate all devices is enabled by default.
To allocate devices based on groups:
Unselect Allocate all devices checkbox.
 Click Apply. Policy Configuration for Device Allocation option appears in the right pane.
 Use the Device Addition option in the right pane to add the devices that are to be managed.
Click Policy Configuration for Device Allocation to select the groups that are to be managed. You can also create new groups and have them managed by LMS.
Alocate al devices
Device management functions
Select the functions that will manage the allocated devices and click Apply.
✓ Inventory, Config and Image Management
Network Topology, Layer 2 Services and User Tracking
✓ Fault Management
IPSLA Performance Management
Device Performance Management
Note: If you disable a function, the function will stop collecting device information. For IPSLA Management, history data will be deleted.
Secondary Credentials
LMS uses either the primary or secondary credentials to access devices. The secondary credentials are used as a failback when the primary credentials fail. Select this check box and click Apply to failback to the secondary credentials.
Fallback to Secondary Credentials
Apply
Proceed to Device Addition

Device Addition

There are multiple ways to add devices into LMS database as described below:

- · Device autodiscovery
- Manually adding devices
- Importing devices

For the purpose of this document, device autodiscovery is shown in Figure 30. For device autodiscovery, select Admin \rightarrow Network \rightarrow Discovery settings.

Figure 30. Options for Device Autodiscovery

	Discovery Settings	Summary	
avigator	Discovery settings	Summary	
chedule			
ottings	Discovery Settings Summary		
rearigs	Module Settings:	Configure	
	Seed Device Settings:	Configure	
	SNMP Settings:	Configure	
	Filter Settings:	Configure	
	Global Settings:	Configure	
	Modules Selected:	LLDP, CDP, Routing Table, ARP	
	Use DCR as Seed List:	No	
	Preferred Management IP:	Use LoopBack Address	
	Preferred DCR Display Name:	Sysname, IP address - Fallback in Order	
	Update DCR Display Name:	No	
	Select a Default Credential Set:	No Default	
	E-mail:		
	Add Discovered Devices to a Grou	p:No	
	Selected Group Name:		
		Configure Start Discovery	

Select the discovery protocol that you would like to use based on your network design. You can select one or multiple discovery protocols (Figure 29).

Figure 31. Selecting Discovery Protocols

		11 Jul 2011, 11:35 UTC
Mode: ADDING	Module Settings	
1. Module Settings 2. Seed Device Settings 3. SWP Settings 4. Rike Settings 5. Global Settings 6. Summary	Hoddle Settings Layer 3 Discovery Protocol Protocol Open Stortes Path First Protocol (OSPF) Open Stortes Path First Protocol (OSPF) Decord Table Varier 2 Discovery Protocol (ULP) Pring Discovery Protocol (ULP) Pring Discovery Protocol (ULP) Charter Discovery Modola Interview Protocol (ULP) Pring Discovery Modola Interview Protocol (PSPP)	
	- Step 1 of 6 - Back Next Finish Cancel	

Click Next to configure seed device settings (Figure 30). You can add one or multiple seed devices.

								11 Jul 2011, 11:38 UTC
Mode: ADDING	Seed Device Settings							
# 1. Module Settings								
Seed Device Settings	Seed Device Settings							
# 3. SNMP Settings	Seed Devices	CDP						
ef 4. Filter Settings	Module Specific ARP (IPv4 Only)							
# 5. Global Settings	-009					Use DCR	as Seed List	
of 6. Summary	Routing Table (IPv4 Only)	File to be Im	Jorted		Browse	📝 Jump Ro	uter Boundaries	
	* Global		-	1000 States and 1		Showin	g 3 records	
				Seed Devices		Hop Count		
			1.	192.168.136.126		5		
			2. 🔳	10.0.252.3		5		
			3. 🕅	10.0.255.76		5		
		-	-			(Dulata)		
						Delete	AQQ	
	- Step 2 of 6 -					Back Next	Einish Cancel	

Figure 32. Adding Seed Devices

Click Next to add SNMP settings (Figure 31).

Figure 33. Adding SNMP Settings

Mode: EDITING	SNMP Settings	11 30 2011, 1139 01C
If 1- Module Settings If 2- Seed Device Settings If 3- SNMP Settings If 4- Filter Settings If 5- Glaboratory	SMMP Settings Samp-V2C Samp-V3 Samp-V2C to Samp-V3 Falback	
ef 6. Summary	SNMPv2 Showing 1-1 of 1 records	
	SNMP Version Target Read Community Timeout Retries Comments	
	1. 🔲 v2t *.*.* ****** 3 1	
	Rows per page 100 - If 1 pages 0000	
	CSelect an item then take an action> Edit Deleter Add	
	- Step 3 of 6 - Back Next. Finish Cancel	

Click **Next** to go to Filter Settings (Figure 32), which is an optional step and can be used if you would like include or exclude specific IP addresses, DNS domains, system objectIDs, or system locations from your discovery process.

Figure 34. Filter Settings

Mode: EDITING	Filter Settings
af 1. Module Settings af 2. Seed Device Settings af 3. SNMP Settings af 4. Filter Settings af 5. Global Settings	Filter Settings Use Filter: IP Address Include/Exclude © Include Devices Exclude Devices
g 6. Summary	Showing 0 records No records No records Delete Add
	- Step 4 of 6 - Back Next Finish Cancel

Click **Next** and the Global Settings page will appear (Figure 35). This step is optional; however, if you skip this step, you will lose the opportunity of choosing the preferred display name, which is Sysname or DNS name, and a few other options.

Sysname (system name of the devices) is introduced in Cisco Prime LMS 4.1 as another option for displaying discovered devices, using sysname in cases where DNS is not available to resolve host names.

Mode: EDITING	Global Settings	
I. Module Settings Seed Device Settings 3. SNMP Settings 4. Filter Settings 5. Global Settings 6. Summary	Clobal Settings Preferred DCR Display Name Sysname DNS Resolvable Host Name Append Domain Name to display name Yes No NOTE: If multiple options are setted; the fallback order will be Sysname, DNS resolvable hostname, and IP address. DCR Administration Settings Update DCR Display Name Seler a Defair (redent) dis film Default	Preferred Management IP Use LoopBack Address Resolve by Name Resolve by SysName None Add Discovered Devices to a Group
	E-mail Notification	Outo All Devices Devices Devices newly discovered during last run Group Name: Select Delete Devices from Group MOTE: If you select the option Toevices newly discovered during last run and entergreated during last run norm on the will be converted.
	- Step 5 of 6 -	Back Next Finish Cancel

Figure 35. Global Settings

Note: If multiple options are selected, the fallback order will be Sysname, DNS resolvable hostname and IP address.

Click **Next** for the final step of this discovery process, which is a summary page (Figure 34) that provides a summary of selections from step 30 to step 35.

Figure 36. Discovery Settings Summary

Inventory > Device Administra	ation > Discovery > Settings		11 Jul 2011, 11:46 UTC
Navigator	Discovery Settings	Summary	
Schedule	Discourse Cathlines Company		
Settings	Model Settings: Seed Device Sattings: Seed Device Sattings: Global Settings: Models Settings: Models Settings: De Chi as Seed List: Preferred Management IP: Preferred Management IP: Preferred Not Display Name: Update COX Display Name: E-the Default Control Setti E-the Default Control Setti E-the Default Control Setti E-the Default Control Setti Setting Name:	Configure Configure Configure Configure Configure Configure ULPP, COP, Rooking Table, ARP No Use LoogBack Address Systems, IP address - Falback in Order No In b Dafauk p: No	

Click **Start Discovery** to start the network device discovery. Cisco Prime LMS will run the discovery based on the discovery protocols that you chose in the previous step and will display all the discovered devices.

User Management

In this section, you can define user roles and, based on the user roles, you can define and add users.

User Roles

Cisco Prime LMS provides system predefined roles and a default role. But you can also create your own roles to fit your organizational needs as well as change the default role. This section shows how to create a customized role. If you don't need to define a custom role, please skip this subsection.

Go to Admin → Getting Started → User Management → Manage Roles and Click Add. See Figure 37

Figure 37. Managing Roles

Variange Roles You can add, copy, edit, and delete custom user roles and set the default user roles. Manage Roles Image Roles Copy Edit Role Description Default Role Image Roles Role Description Default Role Image Roles Image Role Role Description Default Role Image Roles Image Role Image Role Image Role Image Roles Image Role Image Role	Anage Roles You can add, copy, edit, and delete custom user roles and set the default user roles. Manage Roles	Admin > Gett	ng Started					
Namage Roles Role Copy Set as Default Zelit Default Role Role Default Role Role Description Default Role Help Desk Help Desk Role ✓ Network Operator Network Operator Role ✓ Network Administrator Network Administrator Role ✓ System Administrator System Administrator Role ✓	You can add, copy, edit, and delete custom user roles and set the default user roles. Manage Roles Image Roles	lanage Ro	les					
Marage Roles Add Y Filter Role Description Default Role Help Desk Help Desk Role ✓ Network Operator Network Operator Role ✓ Approver Approver Role ✓ Network Administrator Network Administrator Role ✓ System Administrator System Administrator Role ✓	Manage Roles Edit Copy Edit Delete Role Description Help Desk Help Desk Role Network Operator Network Operator Role Approver Approver Role Network Administrator Network Administrator Role System Administrator System Administrator Role	You can ad	d, copy, edit, and delete	e custom user roles an	nd set the de	efault user roles	B.	
Edit Delete Copy Set as Default Add Filter Role Description Default Role Help Desk Help Desk Role ✓ Network Operator Network Operator Role ✓ Approver Approver Role ✓ Network Administrator Network Administrator Role ✓ System Administrator System Administrator Role ✓	Edit Copy Set as Default Add Filter Role Description Default Role Help Desk Help Desk Role ✓ Network Operator Network Operator Role ✓ Approver Approver Role ✓ Network Administrator Network Administrator Role ✓ System Administrator System Administrator Role ✓	Manage Ro	les					- 😵
Role Description Default Role O Help Desk Help Desk Role ✓ O Network Operator Network Operator Role ✓ O Approver Approver Role ✓ O Network Administrator Network Administrator Role ✓ O System Administrator System Administrator Role ✓	Role Description Default Role Help Desk Help Desk Role ✓ Network Operator Network Operator Role ✓ Approver Approver Role ✓ Network Administrator Network Administrator Role ✓ System Administrator System Administrator Role ✓	/ Edit	🔇 Delete 👔 Copy	🥜 Set as Default	🛛 Add	Ϋ Filter		
Help Desk Help Desk Role ✓ Network Operator Network Operator Role ✓ Approver Approver Role ✓ Network Administrator Network Administrator Role ✓ System Administrator System Administrator Role ✓	Help Desk Help Desk Role ✓ Network Operator Network Operator Role ✓ Approver Approver Role ✓ Network Administrator Network Administrator Role ✓ System Administrator System Administrator Role ✓	Role	Des	scription			Default Role	
Network Operator Network Operator Role Approver Approver Role Network Administrator Network Administrator Role System Administrator System Administrator Role	Network Operator Network Operator Role Approver Approver Role Network Administrator Network Administrator Role System Administrator System Administrator Role	O Help Des	k Help	o Desk Role			1	
Approver Approver Role Network Administrator Network Administrator Role System Administrator System Administrator Role	Approver Approver Role Network Administrator Network Administrator Role System Administrator System Administrator Role	O Network	Operator Net	work Operator Role				
Network Administrator Network Administrator Role System Administrator System Administrator Role	Network Administrator Network Administrator Role System Administrator System Administrator Role	O Approve	r App	rover Role				
O System Administrator System Administrator Role	System Administrator System Administrator Role	O Network	Administrator Net	work Administrator Role				
		O System /	Administrator Sys	tem Administrator Role				
O Super Admin Super Admin Role	Super Admin Super Admin Role	O Super Ad	lmin Sup	er Admin Role				

Enter the role name as Myrole, enter some description, and choose the tasks that this role can execute. See Figure 36. Here we are choosing **Reports** and **Monitor**. Through the role-based access control (RBAC) settings, Myrole can perform only the reporting and monitoring functionality of LMS.

Figure 38. Managing Roles

ame: MyRole		
escription: My Custom	er Role	
asks		
earch Input	>	
All Search Re	suits	
V Reports Monitor Configur Configur Admin Work Ce Inventor	ation	

Click OK.

Figure 39. Completed Customized Role

Ma	inage Roles	Orania Calena Dafarilia	97 Filler		
/	Role	Description	Y Fliter	Default Role	
С	Help Desk	Help Desk Role		1	
0	Network Operator	Network Operator Role			
0	Approver	Approver Role			
О	Network Administrator	Network Administrator Role			
О	System Administrator	System Administrator Role			
О	Super Admin	Super Admin Role			
0	Myrole	My Customer Role			

A customized role is now created that can perform only reporting and monitoring of the entire network.

Adding Users

You can also add users to LMS. To add users, go to Admin \rightarrow Getting Started \rightarrow User Management \rightarrow Manage Users and click Add. See Figure 40.

Figure 40. Adding Users

Admin > Getting S Manage Users	itarted			
Manage Users	idit, and delete user	s, and set the authoriza	tion mode for the users.	\$
/ Edit 🗙	Delete 🛛 Add	/ Modify My Profile	Ϋ Filter	
Username	-		Email ID	
🔿 admin			yourusername@example.com	
O guest				

In this case, we are creating a user called joe123. See Figure 41.

Figure 41. Creating User joe123

ser Information	
User Login Details Username:	joe123
Password:	•••••
Email:	joe@cisco.com
Authorization Type	
Select an option: C Full Au Roles Help Desk	Ithorization Enable Task Authorization Enable Device Authorization Device level Authorization Not Applicable
Network Operator	
Approver	
🔲 🔲 Network Administrat	tor
🔲 🗐 System Administrato	pr l
Super Admin Myrole	
Network Level Login Cred	lentials
Username: Password:	Verify Password:
Enable Password:	Verify Password:

Click **OK**. The Manage Users window (Figure 42) appears.

Edit 🔀 Delete 🛛 🗹 Add 🥖 Modify My Profile	e 🕎 Filter	
Jsername	Email ID	
dmin	yourusername@example.com	
pe123	joe@cisco.com	

Figure 42. joe123 Has Been Added to the Users

A new user joe123 has been added with MyRole privileges.

RBAC is also very useful for user-defined groups into which you can group your devices into a group and then assign roles for user, allowing joe123, for example, to manage only that specific user-defined group.

To add a user-defined group, click Admin \rightarrow System \rightarrow Group Management \rightarrow Device and click Create. See Figure 43.

avigator	Device Group Administratio	n		
levice				
ault	Group Administration and Configuratio			
PSLA Collector	- Group Selector	Group Info		
ort and Module	DFM@eset-Ims-41-2			
	E C LMS@eset-Ins-41-2	Group Name:	/LMS@eset-Ims-41-2/User Defined Groups	
	Cisco RO Devices	Type: Description:	User defined groups	*
		Created Bur	Sucham: Wed 22, 3m, 2011 15:20:24 LITC	•
		La but de la		

Figure 43. Adding a User-Defined Group

Add a user-defined group, Cisco RO Devices, by adding the devices that you want to be part of this group.

Once you creat this group, you can use the Role Management setup window and assignuser joe123 to manage the Cisco RO device group with Myrole. See Figure 42.

Figure 44. Assigning Roles to Groups

User Login Details			
Jsername:	joe123		
Password:	•••••	Verify Pa	ssword:
Email:			
Authorization Type			
Select an option: 🔘 Full Auth	orization 🔘 Enab	le Task Authorization	Enable Device Authorization
Roles			
			Defined Groups
🔲 Network Operator			fined Groups
Approver			o RU Devices
🔲 Network Administrator			
🔲 System Administrator			
🔲 Super Admin			
🔲 Se_role1			
V Myrole			
Network Level Login Creder	itials	,	
Jsername:			
		Verify Password	
Password:		verity rassword.	

The next step of the work flow is updating software and devices.

Software and Device Updates

LMS periodically releases software and device package updates to keep your server up to date with all the latest patches. With LMS 4.1, there is a ticker functionality available through which you can quickly install these patches.

To access the ticker function, go to Admin \rightarrow Dashboards \rightarrow System. See Figure 45.

Figure 45. The Ticker Function Allows Quick Installation of Patches



At this stage you do not need to go to the section of software and device updates.

Advanced Configurations

Monitoring

Automonitoring in LMS allows you to select the Link Port groups or All Devices group and monitor the interlink switches automatically. When you want to monitor these groups, pollers are created based on the polling intervals. The polling interval is the duration after which LMS queries the MIB variable on the device. Here the duration is calculated in terms of minutes and hours.

For example, if the polling interval for a poller is set as 15 minutes and the first polling cycle starts at 10:00 a.m., the next polling cycle is scheduled to start at 10:15 a.m.

You can change the polling intervals and select a different interval.

See Monitoring and Troubleshooting with CiscoWorks LAN Management Solution 4.1 for more information.

Fault Management Settings

Managing polling parameters is a key fault management feature in LMS. This feature allows you to perform the following tasks:

- · Viewing polling parameters
- Previewing polling parameters
- Editing polling parameters
- Restoring factory setting polling parameters
- Restoring factory setting polling parameters
- Device polling settings

You can adjust polling parameters only on devices. Port and interface polling is controlled at the device level.

See Monitoring and Troubleshooting with CiscoWorks LAN Management Solution 41 or more information.

Configuration Management

The Template Center in LMS provides you with a list of system-defined templates. These templates contain configuration commands that can be deployed on the devices in your network. These templates are deployed using Deploy Template jobs in LMS.

See Configuration Management with CiscoWorks LAN Management Solution 4.1 for more information.

Inventory and Configuration Management

Business Scenario

As enterprise networks grow ever larger, it becomes a tedious job to manage hundreds or even thousands of devices. With the Inventory and configuration management functions in LMS 4.1, we can address tasks such as:

- How do I keep track of the inventory of devices on my network? How do I generate a customized report that digs out just the inventory information I need?
- How do I keep track of the outdated devices and plan for an equipment upgrade budget? How do I keep track of not only outdated hardware but outdated Cisco IOS Software images?
- How do I keep an archive of the configuration and be able to restore the configurations if there is any misconfiguration? How do I push configurations to multiple devices on my network without doing it onebyone through the CLI? How do I keep track of the changes?
- How do I manage compliance by enforcing configuration policies across the network so everyone is following rules when they configure hundreds of devices?
- How do I automatically upgrade the software images on devices without spending too much time and affecting our business?
- How do I monitor the syslog messages and be automatically notified if something happens?

Configuration Management Overview

LMS consists of many automated features that simplify configuration management tasks, such as performing software image upgrades or changing configuration files on multiple devices Configuration Management in LMS consists of the following major components:

- **Configuration Manager:** Maintains an active archive of multiple iterations of configuration files for every managed device and simplifies the deployment of configuration changes. You can use ConfigEditor to change, compare, and deploy configuration to one device, or use NetConfig to deploy to multiple devices. You can design baseline templates for different configuration needs. You can also specify which action to take after the configuration is deployed.
- **Software Manager:** Simplifies and speeds software image analysis and deployment. You can do an automatic upgrade analysis to help you select the right image. Then use the SWIM feature to import images, stage the image locally or remotely, then deploy to groups of devices.
- Syslog Analysis: Collects and analyzes syslog messages to help isolate network error conditions. You can filter the syslog messages and designate actions based on the messages.
- **Change Audit Services:** Continuously monitors incoming data versus stored data to provide comprehensive reports on software image, inventory, and configuration changes.
- Audit Trails: Continuously monitors and tracks changes made to the LMS server by the system administrator.
- **Compliance Management:** By creating a baseline template, which is essentially sophisticated regular expressions, users can enforce configuration rules to help ensure that the configuration complies with the internal policies or government regulations.

Inventory Management Overview

Inventory Management provides comprehensive device information, including hardware and software details. This information is crucial for network maintenance, upgrades, administration, troubleshooting, and basic asset tracking. The inventory information can also be used by other applications that need access to this same information without the need for additional device queries. Network administrators must often be able to quickly provide information to management on the number and types of devices being used on the network. The more information network administrators have in one central place about all the devices, the easier it is to locate necessary information, resolve problems quickly, and provide detailed information to upper management.

Periodic inventory collection versus periodic inventory polling:

A periodic inventory collection job collects inventory data from all devices (devices in the All Devices group) and updates inventory database. The periodic polling polls all devices to check a certain MIB value to see whether the timestamp has changed. If there is a change in the timestamp, LMS then goes ahead to retrieve inventory changes and collects and updates the inventory database.

Note: Inventory polling consumes much less bandwidth than inventory collection.

The predefined default periodicity of the collector job is once a week, and the predefined default periodicity of the polling job is once a day.

The polling job detects most changes in all devices, with much less impact on your network and on the LMS server.

The Inventory Dashboard (Figure 46) can be accessed by clicking **Inventory** \rightarrow **Dashboards** \rightarrow **Inventory**.

Inventory > Dashboards	> Inventory						11 Jul 2011, 13:42 UT
Audit Trail Informa	ition			✓ 容 ? = □ ×	Software Summary		✓ 睿 ? _ □ ×
No Audit Records Foun	d				Software Version	Count	
Hardwara Summar				v sko m v	Generic Class	8	
Hai Gware Summai	y			× 96 (= 0 A	8.5.1.10000-26	3	
		Cisco Interface	s and Modules		12.2(58)SE1	3	
		Voice and Tele	phony		package	2	
		Unknown			15.1(4)M	2	
	/	TelePresence			12.2(55)SE3	2	
		Svitches and H	lubs		4.2(1)W1(1.42b)	2	
		Non Circo Devi	(a)		15.1(4)MI	2	
					12.2(15)T	1	
					12.2(18)53#7	1	
					User Tracking Summary		✓ 晉 ? 二 □ ×
Device Change Auc	lit			✓ 椰? = 田 X	Number of End hosts		175
Device Name	User Name	Creation Time	Message		Number of Active End hosts		132
NY-3750-5BR.cisco.com	admin	Jul 11 2011 11:43:51	CONFIG_CHANGE		Number of Connected End Hosts		18
NY-3750-58R.cisco.com	admin	Jul 11 2011 10:44:04	CONFIG_CHANGE		Number of Dormant hosts in last 7 days		34
NY-3750-SBR.cisco.com	admin	Jul 11 2011 10:35:41	INVENTORY_CHANGE		Number of Roque hosts in last 7 days		0
NV-2750-SER circo com	admin	3411 2011 10-22-17	CONFIG CHANGE				-

Figure 46. The Inventory Dashboard

Inventory Reports

LMS starts retrieving inventory information based on the default schedule setting. LMS has numerous predefined reports for Inventory. These reports can be viewed by going to **Reports**-Inventory-Hardware. See Figure 47.





The reports include Chassis Slot Details, which provides information on the slots for the chassis-based devices, and the Chassis Slot Summary, among others.

All these reports are generated with a set of predefined query criteria. For example, Software Report will list the software versions based on the categories of the devices. If you want to query a customized list of variables from the inventory, you can use acustom reports template for this as described in the following section.

Some built-in reports are unique in LMS:

- PSIRT Summary report: Introduced in LMS 3.0, this report automates how users track the PSIRT security alert from Cisco. The LMS server can be scheduled periodically to fetch the PSIRT information from cisco.com and correlate to the user's network devices. To run this report, go to Reports→Fault and Event→PSIRT Summary.
- EoS/EoL Hardware report: Introduced along with the PSIRT report, this report works in a similar way to
 automate how users track the end-of-sale/end-of-life status of the network devices. Good for budget
 planning. Some customers schedule it to run every quarter to know how much equipment needs to be
 upgraded.

Custom Reports

To create a customized report (Figure 46) with your particular query variables, such as "the serial number of all c1701 routers," follow these steps:

 Create a custom report template. Go to Reports→Report Designer→Syslog and Inventory→Custom Report Template and click Create.

Figure 48. The Custom Report Templates Window

Reports > Report Designer > Syslog and Inventory	Custom Report Template				11 Jul 2011, 13:50 UT
Navigator	Custom Report Templates				
Inventory	P				
Switch Port				Showing 22 records	
Technology	Template Name 🔻	Report Type	Owner	Last Modified Time	
Fault and Event	1. 🛄 uBR Severity Level 2 (Critical messages) Report	Syslog	admin	Apr 26 2011 21:45:43	
Performance	2. 🛄 UBR Severity Level 0 and 1 (Emergency/Alert messages) Report	Syslog	admin	Apr 26 2011 21:45:43	
Osco.com	3. 🛄 Smart Install	Syslog	admin	Apr 26 2011 21:45:43	
* System	4. 🛅 Sevently Level 2 (Critical messages) Report	Syslog	admin	Apr 26 2011 21:45:43	
Audit	5. Seventy Level 0 and 1 (Emergency/Alert messages) Report	Syslog	admin	Apr 26 2011 21:45:43	
Report Designer User Tracking	6. 📰 Reload Report	Syslog	admin	Apr 26 2011 21:45:43	
Medianet Custom Layouts	7. 🔄 PoE MAX Power Violation	Syslog	admin	Apr 26 2011 21:45:43	
Syslog and Inventory	8. T PDX Denial of Service Report Outgoing TCP or UDP Connections	Syslog	admin	Apr 26 2011 21:45:43	
Custom Report Template	9. T PDX Denial of Service Report Incoming TCP or UDP Connections	Syslog	admin	Apr 26 2011 21:45:43	
Report Settings	10. 🖾 Memory Allocation Failure Report	Syslog	admin	Apr 26 2011 21:45:43	
Report Archives	11. 🗾 IP SLA Threshold violations	Syslog	admin	Apr 26 2011 21:45:43	
	12. 🛅 105 Firewall Denial of Service	Syslog	admin	Apr 26 2011 21:45:43	
	13. 105 Firewall Application Level Intrusion	Syslog	admin	Apr 26 2011 21:45:43	

2. Select the **Inventory** radio button and click **Next** (Figure 49).

Figure 49. Click Next After Selectingthe Inventory Radio Button

Mode: ADDING	Application Selection
□ 1. Select an Application □ 2	Application Selection

3. In the next screen (Figure 50), give a name such as myInventoryReport and choose Private. Click Next.

Figure 50. Naming the Report

Mode: ADDING	Create Inventory Template
If I. Select an Application C. Create Inventory Custom Template Define Inventory Custom Template Rules Use Inventory Custom Template Summary	Template Properties Report Name* (m/InventoryReport) AccossNety: Duble *- Required - Step 2 of 4 - Eack Next Finish Cancel

4. Fill in the values as shown to generate a custom report for chassis serial number and click **Next** and **Finish** (figure 51).

Figure 51. Click Next, then Click Finish to Generate a Report Template

Mode: ADDING	Define Inventory Custom Template Rules
# 1. Select an Application # 2. Create Inventory Custom	Eustom Template Rules I
Template	
3. Define Inventory Custom	Association Inventory Group Attribute Operator Value
Template Rules	Chassis Chassis Serial Number 💌 contains 💌 FDO1415R1GN 💌
Sumary	Chassis:Chassis Model Namexequals:All Add Save Changes Delete Discard Changes
	- Step 3 of 4 - Back Next Frish Cancel

This will generate a template. Now based on this template, you can create a custom report.

- 5. Select Reports → Inventory → myInventoryReport
- 6. Choose the devices, specify the job name and email address and click Finish

Note: Successfully generated reports are stored in the archives. You can access the report archives by selecting **Reports**→**Report Archives**.

Software Image Management

LMS greatly simplifies the work for software image management by building intelligence into the application to help the user pick and access device images from Cisco.com. Follow these steps to perform a software upgrade to your devices.

Step 1. Add images to the repository: Instead of browsing around on Cisco.com trying to find the image file, LMS helps the user to locate the image easily online and adds it into the local repository (Figure 52). You can schedule the download immediately or later.

Select Configuration→Tools→Software Image Management→Software Repository and click Add.

Choose Cisco.com and All devices.

- Note: You can also export the image from the local repository to be used elsewhere.
- Figure 52. Adding Image Files to the Local Repository



- **Step 2.** Create a job for image distribution:Instead of manually loading the images one by one through the CLI, the user can schedule a job to deploy images to a group of devices.The methods of distribution include:
 - **Basic:** This option allows you to select devices and then perform software image upgrades to those devices. Software management checks the current image on the device and recommends a suitable image for distribution.
 - By Devices [Advanced]: This option allows you to enter the software image and storage media for the device that you want to upgrade. The selected image and storage media are validated and verified for dependencies and requirements.
 - **By Images:** This option lets you select a software image from the software image repository and then use it to perform an image upgrade on suitable devices in your network.

• Use Remote Staging: This option allows you to select a software image, store it temporarily on a device, and then use the stored image to upgrade suitable devices in your network. This is helpful when the Resource Manager Essentials server and the devices (including the remote stage device) are distributed across a WAN.

Software Image Baseline Collection

It is recommended that you first import a baseline of all software images running on your network. The baseline imports a copy of each unique software image running on the network (the same image running on multiple devices is imported into the software library only once). The images act as a backup if any of your devices get corrupted and need a new software image or if an error occurs during an upgrade. If some devices are running software images not in the software repository then a synchronization report can be generated for these devices.

To schedule a synchronization report:

- 1. Select Configuration→Tools→Software Image Management→Repository Synchronization. Click Schedule. Enter the information and click Submit.
- 2. Import a baseline of all software images.
- 3. Once the Software Repository Synchronization job has finished successfully, you could create a job to import all software images on your network by performing the following steps:
 - a. Select Configuration→Tools→Software Image Management→Repository Synchronization. Click Add. Select Network and Use Generated Out-of-Sync Report and click Next.
 - b. All running images that are not in the software repository will appear; click **Next**. Enter the job control information and click **Next**, and click **Finish** when completed.

Note: If you have not selected the Use Generated Out-of-Sync Report option, it will take more time to show the software image selection dialog box.

Configuration ArchiveManagement

The Configuration Management tab in Cisco Prime LMS 4.1 hasthree applications: Archive Management, Config Editor, and NetConfig.

Archive Management

The Archive Management application maintains an active archive of the configuration of devices managed by LMS. It provides:

- The ability to fetch, archive, and deploy the device configurations
- The ability to handle syslog-triggered configuration fetches, thereby making sure that the archive is in sync with the device
- The ability to compare and label configurations

Configuration Collection/Polling

The configuration archive can be updated with configuration changes by periodic configuration archival (with and without configuration polling). You can enable this using Admin->Network->Config Collection Settings->Config Collection Settings.

Note: Scheduled collection and polling are disabled by default as the customer's network may have sporadic bursts of traffic and the network management system should not take up the existing bandwidth. It is best for the customer to select the periodic collection and polling.

You can modify how and when the configuration archive retrieves configurations by selecting one or all of the following:

Periodic Polling

Configuration archive performs an SNMP query on the device; if there are no configuration changes detected in the devices, no configuration is fetched.

Periodic Collection

Configuration is fetched without checking for any changes in the configuration.

Configuration Collection Transport Settings

- Default protocols are used for a configuration fetch and deploy.
- Many protocols are used for performing a configuration fetch and deploy. The system provides a default order of protocols that will be used to fetch or deploy the configuration on the device. You can set the protocols and order for Configuration Management applications such as Archive Management, Config Editor, and NetConfig jobs to download configurations and to fetch configurations.

The available protocols are:

- Telnet
- TFTP
- RCP
- SSH
- Secure Copy Protocol (SCP)
- HTTPS

Config Editor

You can use the Config Editor application to perform the tasks listed in Table 4.

Table 4.	Config Editor Tasks
----------	---------------------

Task	Launch Point
Set or change your Config Editor preferences.	Select Configuration→Tools→Config Editor→Edit Mode Preference.
View the list of previously opened files in private or public work areas.	Select Configuration→Tools→Config Editor→Private Configs or Select Configuration→Tools→Config Editor→Public Configs.
Open a configuration file for editing in four ways: • Device and version • Pattern search • Baseline • External location	Select RME → Config Mgmt → Config Editor → Config Editor.
View the status of all pending, running, and completed jobs. You can also create a new job or edit, copy, stop, and delete a job that you have opened.	Select Configuration→Job Browsers→Config Editor.

The LMS Config Editor function can be used to edit a device configuration stored in the configuration archive and download it to the device. The Config Editor tool allows the user to make changes to any version of a configuration file, review changes, and then download the changes to the device.

When a configuration file is opened with Config Editor, the file is locked so that no one else will be able to make changes to it at the same time. While the file is locked, it is maintained in a "private" archive available only to the user who checked it out. If other users attempt to open the file to edit it, they will be notified that the file is already checked out and they can only open a "read-only" copy. The file will remain locked until it is downloaded to the device or manually unlocked within Config Editor by the user who checked it out or by a user that has network administrator and system administrator privileges.

NetConfig

You can use the NetConfig application to perform the tasks listed in Table 5.

Table 5.	NetConfig Tasks
----------	-----------------

Task	Launch Point
 View and create NetConfig jobs using the NetConfig Job Browser. 	Configuration→Job Browsers→NetConfig
 View job details (by clicking the Job ID hyperlink in the NetConfig Job Browser). 	
You can also:	
◦ Edit jobs	
◦ Copy jobs	
 Retry jobs 	
∘ Stop jobs	
 Delete jobs 	
Create and manage user-defined tasks.	Configuration→Tools→NetConfig→User Defined Tasks
Assign user-defined tasks to valid CiscoWorks users.	Configuration→Tools→NetConfig→Assigning Task

The NetConfig function provides a set of command templates that can be used to update the device configuration on multiple devices all at once. The NetConfig tool provides wizard-based templates to simplify and reduce the time it takes to roll out global changes to network devices. These templates can be used to execute one or more configuration commands on multiple devices at the same time. For example, to change SNMP community strings on a regular basis to increase security on devices, use the appropriate SNMP template to update community strings on all devices using the same job. A copy of all updated configurations will be automatically stored in the configuration archive. NetConfig comes with several predefined templates containing all necessary commands. The user simply supplies the parameters for the command and NetConfig takes care of the actual command syntax. These predefined templates include corresponding rollback commands; therefore, if a job fails on a device, the configuration will be returned to its original state.

Create a NetConfig Job to Enable Syslogs on Devices and Configure LMS Server as Receiver

- 1. Go to **Configuration→Tools→NetConfig** and click **Create**.
- 2. Choose Device Based.
- 3. Choose the devices on which you want to enable the syslog functionality from the Device Selector.
- 4. Choose General, choose subselector Syslog, and click Next (Figure 53).

Figure 53. Enabling Syslogs on Devices



5. Click Add Instance (Figure 54).

Figure 54. Adding an Instance

Comm	ion Paramete	rs				
Loggi	ng Host					h
Action:	Add	 Hosts (cor 	nma separate	d): 10.10).10.1	
IOS Pa	arameters					
Loggi	ng On					
Action:	No Change	•				
Loggi	ng Facility					
Action:	No Change	 Parameter: 	auth	•		
Loggi	ng Level					
Buffer	ed					
Action:	No Change	Conditions	Default	•		
Conso	ole					
Action:	No Change	 Conditions 	Default	•		
Monit	or					
Action:	No Change	 Conditions 	Default	•		
Trap						
Action:	No Change	Conditions	Default	•		
				A	pplicable Devices	
				Save	Reset Cancel	-

- 6. Click Save.
- 7. Choose Add from the Action pull-down menu, and enter the IP address of the LMS server where you want the syslogs to be sent.

Change Management Reports

All changes made on the network through LMS are recorded as part of the change audit. If syslogs are enabled on devices, any out-of-band changes made on the devices are also recorded as part of the change audit. Change audit reports can be viewed by going to **Reports** → **Audit** → **Change Audit** → **Standard**.

Topology

Topology Services is an application that allowsyou to view and monitor your network including the links and the ports of each link.

Topology Services displays the network topology of the devices discovered by LMS through topology maps. Besides these maps, the application generates numerous reports that help you to view the physical and logical connectivity in detail.

To launch Topology Services, go to **Configuration→Topology** (see Figures 55 and 56).

e Edit View Reports Tools	<u>W</u> indow <u>H</u> elp			
🗂 Managed Domains		Summary	- Layer 2 View	
Network Views IAN Edge View	Devices 38 Sv	vitches 16	Routers 16	
Unci Display View	Device List			
Carlos Croups	Device Name	IP Address	Device Type	State
Topology Groups	CORE-2	10.0.255.32	NEXUS7010	Reacha
	RTP-NAM-SRE	192.168.1	ciscoProducts.1314	Reacha
	3945-West-1	10.0.7.2	3945	Reacha
	CCM-PUB1.cisco.com	192.168.1	MCS7845-H	Reacha
	SEP1CDF0F76F312	10.7.11.17	ciscoProducts.1003	Reacha
	SEP001DA2392168	10.15.11.1	ciscoProducts.1003	Reacha
	IND-3550-SBR	10.7.10.3	C3524PWRXL	Reacha
	RTP-3945-RBR.yourd	10.0.101.2	3945	Reacha
	3945-East-1	10.0.8.2	3945E	Reacha
	3750-PHY-1	10.0.252.3	C3750-STACK	Reacha
	7206-Core-2	10.0.255.52	7206VXR	Reacha
	7206-Core-1	10.0.255.42	7206VXR	Reacha
Topology Groups	Cat6K-Dist-1	10.0.255.41	C6506-IOS	Reacha
	IND-3560-SBR	10.7.10.1	C3560-24PS	Reacha
	RTP-3750-SBR	10.1.10.1	C3750-STACK	Reacha
	NY-3750-SBR.cisco.c	10.4.10.1	C3750-STACK	Reacha
	VPC-AGG-2	10.0.255.34	NEXUS7010	Unreac
	CCM-SUB1.cisco.com	192.168.1	MCS7845-H	Reacha
	CUPS.cisco.com	192.168.1	MCS7835-H	Reacha
	SIN-3845-RBR	10.0.106.2	3845	Reacha
	BXB-3750-SBR	10.5.10.1	C3750-STACK	Reacha
	3560-DC-1	10.0.252.4	C3560E-24PD	Reacha
	EL 1 0350 0	1015100	AATEA ATAAL	

Figure 55. The Topology Services Window

Figure 56. Network Topology



Template Center

The Template Center in LMS provides you with a list of system-defined templates. These templates contain configuration commands that can be deployed on the devices in your network. These templates are deployed using Deploy Template jobs in LMS.

You can modify the system-defined templates and save the modified templates as user-defined templates. You can also import templates from a client machine, and these templates are stored as system-defined templates in LMS.

The following device and port-level system-defined templates are shipped in LMS:

- Layer 2 Access Edge Interface Configuration
- Access PortChannel Interface
- Identity-Change of Authorization
- CAB-3750-Access-Config
- 6500-access-edge-trusted-endpoint
- Smart Business Architecture (prescriptive guide for setting up midsize or enterprise network, http://www.cisco.com/go/sba)

To access the Template Center, go to Configuration→Tools→Template Center (see Figure 57).



Deploy							11 56 2011, 1
Choose Templates							
Select templates to deploy configuration							
Template Selector				Selecter	0 Total 60	0	
			show All		*	8	
Template Name	Type	Role In Netv	Category	Created By	Scope	-	
3750X 3560X Infrastri SBA	Partial	Access	BN	Osco	Device		
3750X 3560X Infrastri SBA	Partial	Access	BN	Cisco	Device		
Access Switch Global SBA	Partial	Access	BN	Cisco	Device	1	
Branch Creation	Partial	Branch Offic		Tomer Haga	Device		
□ ► Cat 2960S Infrastruct SBA	Partial	Access	BN	Cisco	Device		
Cat6500 Connectivity SBA	Partial	Distribution	BN	Cisco	Device		
Cat6500 Distribution L SBA	Partial	Distribution	BN	Cisco	Device		
Catalyst 2960-S and 3 SBA	Partial	Access	BN	Cisco	Device		
Catalyst 3560-X Platfc SBA	Partial	Access	BN	Cisco	Device		
□ ► Catalyst 3750 Distribu SBA	Partial	Distribution	BN	Cisco	Device		
Catalyst 3750 and 37! SBA	Partial	Distribution	BN	Cisco	Device		
Catalyst 3750G Distrib SBA	Partial	Distribution	BN	Osco	Device		
Catalyst 4500 Access SBA	Partial	Access	BN	Cisco	Device		
							Previous Next Prish Can
	Deploy Closes Templates Select templates to deploy configuration Template Selector Template Selector Template Selector Template Selector Template Selector Template Selector Selector Configuration Configura	Choose Templates Select templates to disploy configuration Template Selector Template Selector 97300 55000 (rinters 58A) 97300 5500 (rinters 58A) 97300	Terplay Clocor: Tereplates Select templates to disploy configuration Templates balector Templates Selector 9 27000 359000 Minketin SBA 9 27000 359000 Minketin SBA 9 27000 359000 Minketin SBA 9 Access Switch Gibble SBA 9 Access Switch Gibble SBA 9 Categot Distribution 9 Categot Distribution 9 Categot Distribution 9 Categot Stribution 9 Categot Distribution SBA 9 Categot 25000 Minites SBA 9 Categot 25000 Minites 9 Categot 27000 Minites 9 Categot 27000 Minites 9 Categot 27000 Minites 9 Categot 27000 Distributes 9	Select templates Select templates to deploy configuration Templates Selector Select templates to deploy configuration Templates Selector 9 37050 0500 chinkatter SBA 9 37050 0500 chinkatter SBA Partial Access 10 Access 11 Access 11 Access 12 Access 13 Access 14 Access 15 Accel Access 16 Access 17 Accester 1700 Deteth	Select templates Select templates to deploy configuration Templates Selector Templates Selector Status 9 3700 30500 finitiants SBA Partial Access Branch Creation Partial Access Partial Access Catalyst 3500 kTrites Partial Access Catalyst 3500 kTrites Partial Access Catalyst 3500 kTrites Partial Catalyst 3500 kTrites Catalyst 3500 kTrites Catalyst 3500 kTrites Catalyst 3500 kTrites Partial Catalyst 3500 kTrites Partial Catalyst 3500 kTrites	Steel Tendets Select templates to deploy configuration Templates Selector Select templates to deploy configuration Templates Selector Show ////////////////////////////////////	Percever Select templates to deploy configuration Template Selector Stow Image: Stow<

The user workflow to deploy the templates is as follows:

- Choose the template to deploy.
- Select devices from the Device Selector and click Next.
- If you have selected port-related templates, the Choose Port Groups pane appears, displaying the Port Selector.
- If you have selected module-related templates, the Choose Module Groups pane appears, displaying the Device Selector.
- Select port groups from the Port Selector and click Next.
- The corresponding template pane appears, allowing you to enter the applicable values for the template.
- Enter the values and click Next.
- The Adhoc Configuration for Selected Port/Device Groups pane appears, allowing you to enter the configuration commands that will be deployed on the selected devices or ports in addition to the commands in the template. The commands that you enter here will not be validated by LMS.
- Click Next.
- The Schedule Deployment pane appears, displaying Scheduler and Job Options details.
- Enter a Job Description, select the Schedule and Job options, and click Finish.
- A notification message appears along with the Job ID. The newly created job appears in the Template Center Jobs.

Job Management

Jobs need to be created for performing archive management, editing of configurations, downloading of configurations, and Cisco IOS/Catalyst OS device image management. All these jobs can be viewed by clicking the links under Configuration-Job Browsers-NetConfig, Configuration-Job Browsers-Software Image management, and so on.

Monitoring

Monitoring Dashboard

Figure 58 Shows the Monitoring Dashboard.



Device Availability Distribution based on average Devi	ce Availability percentage over the	last 1 Hour	✓ 容 ? _ Ⅲ ×	Interface Availabili Distribution based o	ty n average Interface Availabilit	y percentage over the las	it 1 Hour	∯?_⊞X
	All Interfaces are available as per last polied cycle.							
0 - 10 All devic Click here to configure more Pollers.	10 - 50 📑 50 - 90 📑 90 - 101	o nd cycle.		Click here to configure	l o - 10 ■ 10 - 50 ■ 50 All Interfaces are availa more Pollers.	b - 90 🛛 90 - 100	cde.	
Click here to configure more Polers.	10 - 50 🚦 50 - 90 📕 90 - 101	a cycle.	/ 存 ? _ 田 X	Click here to configure High Severity Fault	All Interfaces are availa more Polers.	b - 90 📕 90 - 100	w ≝≣	存? ×
O - 10 All devic Cick here to configure more Polers. Fault Events Summary Events Name	10 - 50 📮 50 - 90 📑 90 - 101 res are available as per last polle Severty	ed cycle.	/存?_日×	Click here to configure High Severity Fault Severity Status	All Interfaces are availa more Polers.	ble as per last polled cyr	ccle.	
0 - 10 Idevic All devic Click here to configure more Poters. Fault Events Summary Events Name Operational/Coven	10 - 50 S0 - 90 90 - 101 res are available as per last polle Saventy Critical	o Indexed and the second secon	/ 存 ? _ 回 X	Click here to configure High Severity Fault Severity Status Active	All Interfaces are availa more Polers.	be as per last polled cyr ble as per last polled cyr Event Name OperationalyC	cle.	存? 田 X Owned By NA
O - 10 Idevic All devic Cick here to configure more Polers. Fault Events Summary Events Name Operational/Covm State/of/Nami	10 - 50 50 - 90 90 - 101 res are available as per last polle Seventy Critical Critical	e eycle.	/存?_= 田 × 6 4	Click here to configure High Severity Fault Severt Status Active Active	All Interfaces are availar more Polers. IS Device Name 10.0.255.72 10.0.255.72	be as per last polled cyr ble as per last polled cyr Event Name OperationalyC OperationalyC	cte. Component Nami Creation Time #-10.0.255.72/4 11-34/2011 14 F-10.0.255.72/4 11-34/2011 14	春? _ 田 × Owned By NA NA
0 - 10 All devic All devic Cick here to configure more Polers. Fadt Events Same Constonal/Covin StateIofNormal Robong	10 - 50 So - 90 90 - 101 res are available as per last polic Soverty Ontcal Ontcal	No. of Devices	/ 存? _ 日 × 6 4 1	Click here to configure High Severity Fault Severity Status Active Active Active	All Interfaces are availa more Polers. Is Device Name 100.255.72 100.010.2	9 - 90 9 9 - 100 ble as per last polled cyr Event Name OperationalyC OperationalyC	Corponent Nani Creaton Time F-10.0.255.72/2 11-342011 14 F-10.0.255.72/2 11-342011 4 F-10.0.1257.72/1 11-3420114	春? _ 田 × Owned By NA NA
O + 10 If devic Cick here to configure more Polyris Fault Events Summary Events Name Operatoral/Covin State/of/Nami Risorig Unresponsive	10 - 50 50 - 90 90 - 101 es are available as per last polic Seventy Ortical Ortical Ortical	e cycle.	/ 存 ? _ 回 × 6 4 1	Click here to configure High Severity Fault Severity Status Active Active Active	All Interfaces are availant more Poles.	ble as per last polled cyr ble as per last polled cyr Event Name OperationalyC OperationalyC OperationalyC	cte. Component Nam Creation Time F=10.0.255.72/4 11-34/2011 14 F=10.0.255.72/4 11-34/2011 14 F=10.0.255.72/4 11-34/2011 14 F=10.0.255.72/4 11-34/2011 14	容?_EX Owned By NA NA NA

Customizing the Monitoring Dashboard Using Portlet

Click the Add Portlet icon as shown get the list of portlets. Choose a portlet, for example, Alert Summary, to add that portlet. See Figure 59.

cisco LAN Management Sol	ution				4	admin Log Out A	xout Sitemap Fee	tback Help	h
My Menu 🔹 Monitor 🔹 Invento	ory 🔹 Configuration 🔹 Reports	🔹 Admin 👻 Wark Cente	rs 🔻						1 S S S
Monitor > Dashboards > Monitoring				Add Portlets	×			and the second second	11 34 2011, 14:5
Device Availability Distribution based on average Devic	ce Availability percentage over the	e last 1 Hour	≠ 停 ? _ 8	Search CiscoWorks Administration	•	iterface Availability perc	entage over the k	ist 1 Hour	⊻ 禱 ? _ ⊞
				Configuration Inventory					
				CPU Utilization Summary	Add Add		7		
0 • 10	10 - 50 📑 50 - 90 📑 90 - 10	0		Custom TOP/Bottom-N Records	Add Add	10-50 50-90	90 - 100		
All device Click here to configure more Poliers.	es are available as per last polk	ed cycle.		Device Performance Management Summary Fault Events Summary High Seventy Faults	Add Add	rfaces are available as	per last polled c	ycle.	
Fault Events Summary			/ 存? _ 1	Highest Jittar					/ 存? 二日
Events Name	Severity	No. of Devices		Highest Latericy	Add	se Name	Event Name	Component Name Creation	Time Owned By
OperationallyDown	Critical			IDCLA Availability	Add	255.72	Operationally	C IF-10.0.255.72/4 11-Jul-20	11 14 NA
StateNotNormal	Critical			Dashboard	Aur	5.11.9	BackupActiva	t IF-10.15.11.9/35 11-Jul-20	11 14 NA
BackupActivated	Critical			IPELA Collector Information	Add	5.11.9	BackupActiva	t IF-10.15.11.9/5J 11-Jul-20	11 14 NA
Flapping	Critical			IDCI & Device Categorization	Auto	5.11.9	BackupActiva	t IF-10.15.11.9/47 11-Jul-20	11 14 NA
Unresponsive	Critical			TPSLA Violation Summary	Add	5.11.9	BackupActiva	t IF-10.15.11.9/44 11-Jul-20	11 14 NA
TOP-N CPU Utilization			/ 存 ? _ 1	Interface Availability	Add				/春?二日
			Time Interval: 1 H					Time 1	interval: 1 Hour

Figure 59. Adding Portlets

Poller Configuration on an Existing Portlet

A few of the portlets may not have any data when the user initially logs in. For example, in the monitoring dashboard, the Top-N Memory Utilization portlet does not have any data.

To configure a new poller, go to **Monitor** \rightarrow **Dashboard** \rightarrow **Monitor**. See Figures 60 and 61.

Figure 60. Configuring a New Poller

My Menu +	Monitor V Inventory V Confi	guration v Reports v	Admin 🔹 Work Centers 💌	-	admin Log Out	About Feedback H	elp (1 - 3	earch 🛒	
Device Availa	Dashboards Monitoring Identity	Troubleshooting Tools NetShow • Troubleshooting Workflows	face Availa	bility			,	01 Aug 2011, 14:23 U 春? 田 ×	
No data is availa Alerts Summ	EnergyWise Diagnostic Tools Embedded Event Manager •	Min-RMON VRFL te * Topology Services Performance Settings Setup *		ta is available.Clickhere to configure Pollers Please check HUMPortal.log for more details					
Alerts Type Discrepancies	Generic Online Diagnostics	Setup • SNMP Traps • Syslog •	Receiver Groups	rity Status Active	Device Name 10.0.101.2	Event BackupAc.	Component	Creation 01-Aug-20	Owned By
Best Practices High Severity F	Ferformance TrendWatch			Active	10.0.105.2	Operatio	IF-10.0.105	28-Jul-201	NA
S0,S1,S2 Syslo IPSLA Violation	g Alerts s		0 0	Active Active	10.0.105.2	Operatio	CARD-10.0	28-Jul-201 28-Jul-201	NA NA
Performance T	hreshold Violations		0 0	Active	10.0.106.2	Operatio	IF-10.0.106	01-Jul-201	NA

Figure 61. Configuring the Poller to Start Memory Utilization

Events Name	Severity	No. of Devices						
OperationallyDown	Critical		8					
StateNotNormal	Critical		2					
Unresponsive	Critical		1					
BackupActivated	Critical		1					
Duplicate	Critical		1					
TOP-N CPU Utilization								
TOP-N Memory Utilization	Pollers Please check	ノ 袋	? _ ⊞ X					
the data to an an an or of the of the gala								

Click the **here** link to configure the poller to get the memory utilization polling started. You need to create a poller for memory utilization (which is not created by default). See Figures 62 and 63.

Figure 62. Creating the Poller

te	er:[All		Show						@
	0	■ Poller Name ▼	Interval	No. of Devices	No. of Templates	Status	Missed Cycles	Poll Start Time	Show Poll End Time	Poller Type
1	. [MemoryPoller	5 Mins	31	1	Active with Errors (153)	0	Mon, Jul 11 2011, 14:56:15	Mon, Jul 11 2011, 14:56:15	Historic
2	. [Link Ports_Interface Uti	15 Mins	27	1	Active with Errors (543)	0	Mon, Jul 11 2011, 14:59:00	Mon, Jul 11 2011, 14:59:00	System
3	. [Link Ports_Interface Err	15 Mins	27	1	Active with Errors (3248)	0	Mon, Jul 11 2011, 14:59:00 UTC	Mon, Jul 11 2011, 14:59:00 UTC	System
4	. [Link Ports_Interface Ava	15 Mins	27	1	Active	0	Mon, Jul 11 2011, 14:59:00 UTC	Mon, Jul 11 2011, 14:59:00 UTC	System
5	. [EnergyWise Poller	15 Mins	2	2	Active with Errors (50)	0	Mon, Jul 11 2011, 14:48:00	Mon, Jul 11 2011, 14:48:00	Historic
6	. [All Devices_Device Avail ability	5 Mins	44	1	Active	0	Mon, Jul 11 2011, 14:55:00	Mon, Jul 11 2011, 14:55:00	System
7	. [All Devices_CPU Utilizat	5 Mins	43	1	Active with Errors (33)	0	Mon, Jul 11 2011, 14:57:30	Mon, Jul 11 2011, 14:57:33	System

Figure 63. Adding Memory Utilizaton to the Poller

ode: ADDING 1. Select Data Source and	Select Data Source and Templat	tes	11 34/2011, 15/
Templates	Data Source and Templates		
2. Select Instances 3. Poller Summary	Select Data Source Port Groups Port Groups	Poller Details Name *: MEM	Poling Interval: 5 Minutos
	< <search input="">> → D</search>	Templates *	
	AI Search Results Selection	Available Templates	Selected Templates
	Classical Control of the co	CPU URbatton CPU URbatton CPU URbatton CPU CPU URbatton CPU	Add >>
	State Jros Ser Sch-PUBLisco com Sch-SUBLisco com sected	Poller Preferences Pol al Instances	Threshold Only
	- Required		
	- Step 1 of 3 -		Back Next Frich Cancel

Once the poller is created the portlet will be populated with the Top-N memory utilization data.

Fault Management

Business Scenarios

On a daily basis, network administrators face many challenges to maintain a healthy running network to support business needs. They constantly ask questions like:

- · How do I quickly and easily detect, isolate, and correct network faults?
- How do I monitor not only up and down status, but also potential problems?
- How do I provide valuable insight into the relative health of a device and the network?
- · How do I address problems before network service degradation affects users?
- · How do I minimize downtime and service degradation?

Cisco Prime LMS 4.1 proactively monitors the network for indicators of device or network faults, helping enable the network administrator to know exactly where the problem is and what to fix, thus avoiding costly network service degradation. LMS has the built-in intelligence to determine what variables and events to look for to determine the health of a Cisco device, without user intervention, for true fault management.

Cisco Prime LMS uses SNMP polling and SNMP traps to discover and display real-time faults. LMS provides rules to analyze events that occur and help determine when a probable fault has occurred on Cisco devices. It allows you to configure immediate notifications on certain types of faults and stores events and alerts for 31 days in the fault history.

LMS already knows which MIB variables to poll for each different device to determine the status and health of the device. The necessary threshold values have also been predefined based on extensive testing.

Fault Monitor

LMS Fault Monitor is a centralized browser where you can view the information on faults and events of devices in a single place.

A fault refers to a problem in the device or in the network. Examples for faults include Device Down, Link Down, and High Utilization.

Fault Monitor collects information on faults and events from all devices in realtime and displays the information by a selected group of devices. It allows you to own the faults or clear them. You can also annotate the devices.

Fault Monitor has two tabs: Device Fault Summary View and Fault View. It provides a launch point for Event Monitor and event forensic data collected.

To view the faults, navigate to **Monitor→Monitoring Tools→Fault Monitor** (Figure 64).

Figure 64. The Device Fault Summary

All Devices	Device Fault Summary	Faults View					
	Devices						🚸 🖨 💀 🍇 🗸
	🔁 Annotate 📑 Even	t Monitor 🛛 Filter					
	8 2	Device Name	Device IP	Туре	0	V 8	Last Updated Time
	• •	10.0.255.72	10.0.255.72	Routers	15	0 0	11-3.4-2011 15:12:56
	0 0	10.15.11.9	10.15.11.9	Routers	22	0 0	11-3.4-2011 15:12:49
	0 0	10.0.101.2	10.0.101.2	Routers	16	0 0	11-3.4-2011 15:12:44
	0	sjo-19-fab-a.cisco.com	192.168.138.11	Switches and Hubs	0	0 0	11-3.4-2011 15:05:49
	0 •	10.0.1.2	10.0.1.2	Switches and Hubs	1	0 0	08-Jul-2011 13:26:00
	0 0	10.0.255.41	10.0.255.41	Switches and Hubs	2	0 0	08-Jul-2011 13:25:53
	0 0	10.0.255.52	10.0.255.52	Routers	13	0 0	01-34-2011 21:51:35
	:0 0	10.0.106.2	10.0.106.2	Routers	19	0 0	01-3ui-2011 13:33:36
	0 0	192.168.138.206	192.168.138.206	Voice and Telephony	1	0 0	01-34-2011 10:38:25
	•			***			
	Faults for 10.0.255.72			*****			🔶 🗅 📽 🁙 🗸
	🔏 Own It 🛭 🖌 Clear	🚰 Annotate 🛛 Notify 📋 Event Monitor	∀ Filter				
	0 🐥 💪 🕻	Event Name	Component M	lame	Last	Updated Time	 Owne
		OperationallyDown	IF-10.0.255.7	2/47 [Se0/0/0:15]	11-3	ul-2011 15:12:5	6 N/A
		OperationallyDown	IF-10.0.255.7	2/48 [Se0/0/0:16]	11-)	4-2011 15:12:4	5 N/A
		OperationallyDown	IF-10.0.255.7	2/49 [Se0/0/0:17]	11-)	ul-2011 15:12:3	5 N/A
		Operational/Opwn	IF-10.0.255.7	2/35 [Se0/0/0:3]	11-)	4-2011 15:12:2	5 N/A
		all a la l					

In figure 64, the top portion shows the devices. By clicking in any row, the bottom portion of the window shows the faults from the selected device.

To see all the faults, click the **Fault View** tab (Figure 65).

Figure 65. The Faults View Tab

A Conces	Device Fault Sum	ridry routs vew					-
	Faults					10	11 9 8.
	🔒 Own It 🕑 Gi	lear 📴 Annotate 🖂 Notify 👖 Event	Monitor PRiter				
	08 2	Event Name	Device Name	Device IP	Component Name	Last Updated Time	• Owne
		OperationallyDown	10.0.255.72	10.0.255.72	IF-10.0.255.72/44 [Se0/0/0:12]	11-3ui-2011 15:14:25	N// *
		OperationallyDown	10.0.255.72	10.0.255.72	IF-10.0.255.72/45 [Se0/0/0:13]	11-Jul-2011 15:14:06	N//
		OperationallyDown.	10.0.255.72	10.0.255.72	IF-10.0.255.72/46 [Se0/0/0:14]	11-Jui-2011 15:13:45	N// E
		OperationallyDown	10.0.255.72	10.0.255.72	IF-10.0.255.72/32 [Se0/0/0:0]	11-3ui-2011 15:13:25	N//
		OperationallyDown	10.0.101.2	10.0.101.2	IF-10.0.101.2/14 [Se3/0:0]	11-34-2011 15:13:23	N//
		OperationallyDown	10.0.255.72	10.0.255.72	IF-10.0.255.72/33 [Se0/0/0:1]	11-34-2011 15:13:15	N//
		OperationallyDown	10.0.255.72	10.0.255.72	IF+10.0.255.72/34 [Se0/0/0:2]	11-34-2011 15:13:05	N//
	: 🗆 😐 📑	OperationallyDown	10.0.101.2	10.0.101.2	IF-10.0.101.2/15 [Se3/0:1]	11-34-2011 15:13:03	N//
	i o o 🛅	OperationallyDown	10.0.255.72	10.0.255.72	IF-10.0.255.72/47 [Se0/0/0:15]	11-Jul-2011 15:12:56	N//
	00 -	BackupActivated	10.15.11.9	10.15.11.9	IF-10.15.11.9/33 [Se1/0/0:2]	11-34-2011 15:12:49	N//
		OperationallyDown	10.0.255.72	10.0.255.72	JF+10.0.255.72/48 [Se0/0/0:16]	11-34-2011 15:12:45	N//
	O O 0	OperationallyDown	10.0.101.2	10.0.101.2	IF-10.0.101.2/16 [Se3/0:2]	11-Jul-2011 15:12:43	N//
		OperationallyDown	10.0.255.72	10.0.255.72	IF-10.0.255.72/49 [Se0/0/0:17]	11-3ui-2011 15:12:35	N//
		OperationallyDown	10.0.255.72	10.0.255.72	IF-10.0.255.72/35 [Se0/0/0:3]	11-34-2011 15:12:25	N//
		OperationallyDown	10.0.101.2	10.0.101.2	IF-10.0.101.2/17 [Se3/0:3]	11-3ui-2011 15:12:22	N//
		OperationallyDown	10.0.255.72	10.0.255.72	IF-10.0.255.72/50 [Se0/0/0:18]	11-30/-2011 15:12:15	N//
		OperationallyDown	10.0.255.72	10.0.255.72	IF-10.0.255.72/51 [Se0/0/0:19]	11-34-2011 15:12:05	N//
		OperationallyDown	10.0.101.2	10.0.101.2	IF-10.0.101.2/18 [Se3/0:4]	11-3ui-2011 15:12:03	N//
		OperationallyDown	10.0.255.72	10.0.255.72	IF-10.0.255.72/36 [Se0/0/0:4]	11-3ui-2011 15:11:54	N//
		Operational Opun	10.0.255.72	10.0.265.72	15 10 0 255 72/52 [section/0/20]	11.14 0011 16-11-46	hill

In this window, you can clear, own, notify, or annotate an event.

- Own it: Changes the event status to Acknowledged
- Clear: Clears and deletes alarms and events
- Annotate: Suspends polling and trap processing on the device or device component by opening a Detailed Device View (DDV), from which you can perform the suspend command
- Notify: Sends email notification of the alert

By selecting a fault and choosing Notify you can send an email for this fault to an email recipient.

Clicking Event Monitor, by default, shows the Fault History, which is a 24-hour fault history report.

Note: Network devices have to be configured to send syslogs and traps to the LMS server to receive, process, and create faults and events.

Performance Monitoring

Business Scenarios

For network administrators, monitoring the network is an essential requirement in their network management tools. Not only do they need to be able to monitor any MIB object on the networkbut they also need to have a meaningful reporting capability that shows the top issues on the network and proactively provides alerts when things happen. They also need to keep track of the trends of network events to understand the network in a dynamic environment.

Cisco PrimeLMS provides organizations with:

- · CPU, memory, Interface/portmonitoring for utilization and availability levels
- · Support for system-defined MIB templates that facilitateeasy polling setup
- The capability for users to create custom MIB templates
- · Historical reporting on a daily, weekly, monthly, and annual basis
- Threshold breach event notification, reporting, and event handler support
- Comprehensive reporting such as Device Dashboard, Custom Reports, Top-N/Bottom-N Reports
- · Historical trending on a daily, weekly, monthly, and annual basis

Creating Thresholds and Notifications

Select Monitor→Threshold Settings→Performance and click Create (see Figure 66).

Figure 66. Creating and Configuring Thresholds

Threshold Name:* CPUJTIL Terreshold Name:* CPUJTIL Terrejake Name:* CPU Utilization	● Instance Selector ● Port Group Selector ● Device Group Selector < <search input="">> → の All Search Results Selection</search>
Variable Name:** cpmrCPUTotalSmin reshold Criteria Condition: >= Value: **60 No.of Violations: **0 Severity: iCritical Conditions: >= Conditions: >=	
Send Frank to:	
	f shint(s) selected

Workflow for Creating a Threshold

- Choose the variable from the template that you need to set the threshold on.
- Define the condition: threshold value, severity.
- Define the action email, trap, or syslog generation if the threshold condition occurs.
- Choose the device where you want to monitor this threshold.

Understanding the Templates

System-Defined Templates

System-defined templates are logical groups of MIB objects users want to poll. You can view the available LMSsystem-defined templates by selecting **Monitor** \rightarrow **Performance Settings** \rightarrow **Setup** \rightarrow **Templates** (see Figure 67).

Figure 67. LMS System-Defined Templates

utomonitor						0
llers	Filter: A		Show			
mplates					Showing	11 record
		Template Name 4	No. of MIB Varibles	No. of Pollers Associated	Created by	
	1. 🕅	CPU Utilization	1	1	System	-
	2. 🕅	Device Availability	1	1	System	
	3. 🕅	EnergyWise Device Power Usage	2	1	System	
	4. 🕅	EnergyWise Port Power Usage	2	1	System	
	5. 🕅	Environmental Temperature	1	0	System	11
	6. 🕅	Interface Availability	1	1	System	
	7. 🕅	Interface Errors	4	1	System	
	8. 🕅	Interface Utilization	3	1	System	
	9. 🕅	Memory Utilization	2	1	System	-
	t	Select an item and then take an action		Export Delete Ed	t Copy I Import	Create

System-defined templates support all Cisco devices that support the following MIB files:

- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENVMON-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PROCESS-MIB
- ENTITY-MIB
- OLD-CISCO-CHASSIS-MIB
- RFC1213-MIB
- IF-MIB
- CISCO-POWER-EHTHERNET-EXT-MIB
- POWER-EHTHERNET-MIB
- CISCO-RTTMON-MIB

User-Defined Templates

Users can also create their own templates to poll MIB objects they are interested in. To create a template, go to **Monitor**->**Performance Settings**->**Setup**->**Templates** and click **Create**.

In this example, we will create a template to poll the temperature MIB objects using the CISCO-ENVMON-MIB (Figure 68).

Mode: ADDING	Select MIB Variables
I. MIB Variables	MIB Variables
2. MIB Alias Name	Template Name *: ENVMON Show Mib: CISCO-ENVMON-MIB
	All Search Results Selection
	□ D
	CiscoEnvMonPresent CiscoEnvMonVotageStatusTable CiscoEnvMonTemperatureStatusTable CiscoEnvMonTemperatureStatusTable
	CiscoEnvMonFanStatusTable CiscoEnvMonSupplyStatusTable
	Note: Only Integer type Variables will be shown in MIB tree
	- Kedureu
	- step 1 of Z - Back Next Finish Cancel

Figure 68. Creating a Template to Poll the Temperature MIB Objects

Pollers - How to Create

After you get the templates to poll the MIB objects in which you are interested, create a poller to poll the MIB objects on a specified schedule.LMS provides some system-defined pollers as shown in Figure 69.

Select Monitor→Performance Settings→Setup→Pollers and Click Create.

Figure 69. Creating a Poller to Poll the MIB Objects on a Specified Schedule

itor										0
	Filter: All			Show						
5									Showi	ng 7 records
	Pol	er Name 🔻	Interval	No. of Devices	No. of Templates	Status	Missed Cycles	Poll Start Time	Poll End Time	Poller Type
	1. 📰 Memo	ryPoller	5 Mins	31	1	Active with Errors (155)	0	Mon, Jul 11 2011, 15:26:15 UTC	Mon, Jul 11 2011, 15:26:15 UTC	Historic
	2. 🛄 Link P	orts_Interface Uti n	15 Mins	27	1	Active with Errors (543)	0	Mon, Jul 11 2011, 15:14:00 UTC	Mon, Jul 11 2011, 15:14:00 UTC	System
	3. 🕅 Link P ors	orts_Interface Err	15 Mins	27	1	Active with Errors (3248)	0	Mon, Jul 11 2011, 15:14:00 UTC	Mon, Jul 11 2011, 15:14:00 UTC	System
	4. 🕅 Link P	orts_Interface Ava	15 Mins	27	1	Active	0	Mon, Jul 11 2011, 15:14:00 UTC	Mon, Jul 11 2011, 15:14:00 UTC	System
	5. 💹 Energ	yWise Poller	15 Mins	2	2	Active with Errors (50)	0	Mon, Jul 11 2011, 15:18:00 UTC	Mon, Jul 11 2011, 15:18:00 UTC	Historic
	6. 🕅 All De ability	vices_Device Avail	S Mins	44	1	Active	0	Mon, Jul 11 2011, 15:25:00 UTC	Mon, Jul 11 2011, 15:25:00 UTC	System
	7. 🛄 All De	vices_CPU Utilizat	5 Mins	43	1	Active with Errors (33)	0	Mon, Jul 11 2011, 15:27:30 UTC	Mon, Jul 11 2011, 15:27:30 UTC	System
	℃Select	an item and then take a	n action>			De-activate Activ	/ate Delete	Edit Clear Missed Cycle	es I Clear Falures	Create

Here, we will create a poller called myCustomPoller, which polls the selected two devices using the system-defined CPU Utilization template. The setup options include poller name, devices, template, and polling interval (Figure 70).

Figure 70. Creating a Custom Poller

de: ADDING	Select Data Source and Templat	es			
Select Data Source and Templates	Data Source and Templates				
Select Instances	Select Data Source *	Dellas Datala			
L Poller Summary	Device Device Groups Port Groups	Poller Decails	Name *: myCustomPoller	Poling Interval: 5 Minutes	
	< <search input="">> → P</search>	Templates *	4		_
	All Search Results Selection	Available Templates		Selected Templates	
		EnergyWise Port Power Environmental Temperal Interface Availability Interface Errors Interface Utilization Memory Utilization POE PORT Utilization Add User Defined Temp	a Autos	dd >> Remove	
	CALFUEI Lisco com	Poll al Instances		Threshold	d Only
	- Required				

Choose the instances from the next screen and click Next.

The poller, myCustomPoller, appears in the list of pollers (Figure 71).

Figure 71.	myCustomPoller Is Added to the List of Pollers
------------	--

vigator	List of Pollers								
tomonitor									(
llers	Filter: All		Show						
mplates								Show	ng 8 recor
	Poller Name 🔻	Interval	No. of	No. of Templates	Status	Missed Cycles	Poll Start Time	Poll End Time	Poller
	1. myCustomPoller	5 Mins	1	1	Active	0	Schedule to start before Mon, Jul 11 2011, 15:36:05	Yet to be Started	Historic
	2. MemoryPoller	5 Mins	31	1	Active with Errors (155)	0	Mon, Jul 11 2011, 15:26:15 UTC	Mon, Jul 11 2011, 15:26:15 UTC	Historia
	3. E Link Ports_Interface Uti	15 Mins	27	1	Active with Errors (543)	0	Mon, Jul 11 2011, 15:29:00 UTC	Mon, Jul 11 2011, 15:29:00 UTC	Syster
	4. C Link Ports_Interface Err	15 Mins	27	1	Active with Errors (3248)	0	Mon, Jul 11 2011, 15:29:00 UTC	Mon, Jul 11 2011, 15:29:00 UTC	Syster
	5. E Link Ports_Interface Ava	15 Mins	27	1	Active	0	Mon, Jul 11 2011, 15:29:00 UTC	Mon, Jul 11 2011, 15:29:00 UTC	Syster
	6. 🔄 EnergyWise Poller	15 Mins	2	2	Active with Errors (50)	0	Mon, Jul 11 2011, 15:18:00 UTC	Mon, Jul 11 2011, 15:18:00 UTC	Histori
	7. Al Devices_Device Avail	5 Mins	44	1	Active	0	Mon, Jul 11 2011, 15:30:00 UTC	Mon, Jul 11 2011, 15:30:00 UTC	Syster
	8. All Devices_CPU Ublizat	5 Mins	43	1	Active with Errors (33)	0	Mon, Jul 11 2011, 15:27:30 UTC	Mon, Jul 11 2011, 15:27:30 UTC	Syster
	*Select an item and then take	an action>			De-activate Activ	/ate Delete	Edit Clear Missed Cvd	les I Clear Falures	Creat

IPSLA Monitoring

Business Scenarios

Managing mission-critical networks has become an integral component of today's businesses. Customers no longer see the IP network as an unreliable infrastructure on which to build their business. Internet service providers (ISPs) and even internal IT departments now have to offer a defined level of service - a service-level agreement (SLA) - to provide their customers with a degree of predictability. How to measure network response time, determine device availability, resolve connectivity issues, analyze response time patterns, and provide critical reports, both real time and historical, have taken on an even higher priority.

Cisco Prime LMS 4.1 allows generation of IP SLA reports using Cisco IOS IP SLA technology to monitor the endto-end performance of multiprotocol networks. Using IP SLA, Cisco Prime LMSmeasures and displays five key network performance statistics between a source and a target device. These five statistics include latency, availability, jitter, packet loss, and errors.

SLA was formerly known as RTR or SAA. For more information on Cisco IOS IP SLA, visit <u>http://www.cisco.com/go/ipsla</u>.

Workflow for the IPSLA Monitoring

To use LMS for performance management, users need to define collectors to gather the performance data. A collector is made of four components.

- Source router: Originating point from which LMS makes latency and availability measurements. This is
 where the LMS server uses SNMP to configure Cisco IOS IP SLAs. A source router must run Cisco IOS
 Software with the IP SLA feature.
- Target router: Destination of the source router operations (IP SLA measurements) from which response data should be collected. A target can be an IP host, another Cisco IOS device with IP SLA, or a Systems Network Architecture (SNA) host.
- Test operation: The traffic test operations simulate actual network traffic for a specific protocol. For example, to measure the latency for a voice-over-IP (VoIP) session, an Enhanced UDP test operation is created and defined to send a series of 60-byte UDP packets with a specified type of service (ToS) value and target port number.
- Collection schedule: A collector can be scheduled to run at any point in time, or continuously over any time interval. This flexible scheduler makes IP SLAs suitable for both service-level monitoring and troubleshooting.

The workflow for IPSLA management is illustrated below:



Figure 72. IPSLA workflow

As in this workflow diagram, we define the collector from step 1 to step 5. In the first and second steps, the source router and target device are defined. For Cisco IOS devices, we need to turn on IP SLAs in the Cisco IOS Software.

In step 6, IP SLAs in the source router generate the synthetic tests and measure latency/response time. The IPM server will then poll the collectors to collect test results and generate the results in real-time or historical reports.

The following sections will discuss each step in detail.

Source Router and Target Device

The first thing for the user to do is to select the source router and target device. For example, to measure the response time between clients and an application server, the source router will be a Cisco IOS router running software version 11.2 or later on the same segment where the application server will be placed. The target device is placed on the same segment where many clients would access the application server.

Define an Operation

LMS has a number of built-in test operations. Following is a list of the built-in test operations:

- Echo
- Path Echo
- UDP Echo
- ICMP Jitter
- UDP Jitter
- VoIP Post Dial Delay
- VoIP Gatekeeper Registration Delay
- RTP
- DNS
- DHCP
- HTTP
- FTP
- DLSw
- TCP Connect

Finally we tie together the four components of the collector, that is, source and target devices, test operation, and schedule by creating a collector at **Monitor**->**Performance Settings**->**IPSLA**->**Collectors**. Click **Create**. See Figures 73 and 74.

Figure 73. Collector Management window

Monitor > Performance Settings > IPSLA > Collectors										11 A	ul 2011, 15:35 UTC
Navigator	Collector Management										
Collectors											0
Operations	E Coperation Based Groups	Collector	List	1766210	-						
Outage Settings	E Cuser Defined Groups	Filter : Al		Fite						Showing 1	-3 of 3 records
Devices			Collector 🐔	Source	Target	Operation	VRF	Start Date	End Date	Col Type	Status
		1. 🖂	Secondary_DNS_192.168.138 .135_DefaultDNS	RTP-3945-RBR.yo urdomain.com	192.168.138.135	DefaultDNS	Not Applicable	Jun 30, 2011	Forever	Historical	Running
		2 2.	NY-to-LA-Voice_LA-2921-RB R_Default160ByteVoice	NY-2911-R8R	LA-2921-R8R	Default160ByteVoic e	Not Applicable	Jun 30, 2011	Forever	Historical	Running
		3. 🖽	LA_DHCP_Availability_Defa ukDHCP	LA-2921-R6R	Not Applicable	DefaultDHCP	Not Applicable	Jun 30, 2011	Forever	Historical	Running
		E R	ows per page: 10 💌						KCGo to page:	1 of 1 pa	ges Go >>1
	List Collectors	SELECTOR									
	1Select an Rem	then take an act	cn→		View Graph	Edit Delete E	eport [Monitor]	Start Stop I	Import Reco	nfgure Cre	ato

Figure 74. Adding a Collector in the Collector Configuration Window

Mode: ADDING	Collector Configuration		
D 1. Collector			
2. Select Collector	Collector Configuration		
3. Schedule	Collector Information		
D 4. Summary	Collector Name*: ICMPCollection		
	Description:		
		1.04	
			s - 102
	Source Devices	Target Devices	Operations
	<«Search Input»»	< <search input="">></search>	All Selection
	All Search Results	All Search Results Selection	E Operations
	E C C All Devices	E All Devices	E DHCP
	● ♥3560-DC-1	E 33560-DC-1	DLSW
	3750-PHY-1	3750-PHY-1	E CONS
	© 17206-Core-1	3945-East-1.cisco.com	Echo Echo
	© 🐨7206-Core-2	3945-West-1	GatekeeperRegistrationDelay
	BXB-2921-RBR.yourdomain.	7206-Core-1	
	BXB-3750-SBR	206-Core-2	DefaultiCMPJitter
	Catok-Dist-1	BXB-2921-RBR.yourdomain.c	
	© @FI 4.3750.2	CCM-PI PI cisco com	
	© \$FL4-37505-1		
	< <u> </u>	1 device(s) selected	
		,	
	ColortV/R		
	Source Interface (IPAddress)	Note: * - Required Field	
	- Sten 1 of 4 -		
			Back Next Finish Cancel

After the collector is created, you can schedule the collector to run so that it collects the Internet Control Message Protocol (ICMP) jitter matrix.

Reports

Reports Management in Cisco Prime LAN Management Solution 4.1 provides a single launch point for all the reports that can be generated and viewed in Cisco Prime LMS 4.1.

All the reports have been grouped under various headings based on the information displayed.

• Inventory

This section of reports contains reports pertaining to devices, hardware, End-of-Sale (EoS) and End-of-Life (EoL).

Switch Port

This category of reports contains reports such as switch capacity reports, switch port summary reports, and utilization history (over specified time).

Technology

These are reports specific to the Cisco IOS technologies such as EnergyWise, Identity, Powerover Ethernet (PoE), VRF Lite.

Fault and Event

These contain threshold violation, device fault, syslog, and PSIRT reports.

• Performance

These contain CPU utilization, memory utilization, interface utilization, interface error, and IPSLA reports.

- Cisco.com
- System

These contain:

- Reports such as the number of users logged in, collection details, and so on
- Configuration file change reports
- Twenty-four-hour change report: All configuration changes in the last 24hours
- Audit

Change audit reports show software image distribution and download history for software changes made.

Report Designer

As the name indicates, this is a tool to generate custom reports, especially for syslogs and inventory.

• View Report Archives

The report output that is created from a scheduled report is stored in the reports archive. The archive displays the list for completed report jobs, and you can view or delete them (Figure 75).

Figure 75. A List of Completed Report Jobs Is Available in the Reports Archive



Report Generation and Viewing Paradigm

Use case: We want to generate a detailed hardware report for a few devices. See Figures 76 and 77.



My Menu 👻 Monitor 👻	Inventory 🔻 Configuratio	n 🔻 Reports 👻 Admin 👻 W	vork Centers 🔻		분습
Admin > Getting Started Getting Started with LMS CiscoWorks LAN Managemen administer Cisco networks. C Infrastructure. New Features in LMS 4.1	t Solution (LMS) provides yo JiscoWorks Getting Started	inventory Detailed Device Device Attributes 24-hour Inventory Change Hardware Manageme Chassis Stot Details Software Chassis Stot Symmary Gra User Track Chassis Summary Gra	Switch Port Capacity Ports • Recently Down Reclam • Jary bon History ph	Cechnology EnergyWse Identity Medianet PoE VLAN VRF-Lite	Fault and Event Best Practices Embedded Event Manager Syslogs Generic Online Diagnostics Syslogs History PSIRT Summary Syslog Threehold Violation
Improved Usability	💋 EnergyWise	Device	ummary act Connection	ANI Server Analysis Data Collection Metrics	Change Audit
Identity	S Monitoring	Interface Hardware Componen IPSLA Det Hardware Summary C	it Summary _{e Device} Graph rt Settings	Device Support Status 💌	System Device Administration
📓 Auto Smartports	😨 Smart Install	IPSLA Sum Multi Service Port Poller EoS/EoL Hardware	t Publish Path	Users Report Archives	IPSLA Performance
<u> Report Center</u>	🧳 Enhanced Trou	Custom IPSLA System Summary 💌		Inventory and Syslog IPSLA	Inventory and Config
💥 Template Center	👥 Local CiscoWor	Report Designer		User Tracking	

Figure 77. Select the Devices You Want to Include in the Report

cisco LAN Management Solu	ition	admin Log Out About Feedback Help 🕞 💌 Search	*
My Menu 🔻 Monitor 👻 Invento	ry 🔻 Configuration 👻 Reports 👻 Admin 👻	Work Centers 👻	표 습
Reports > Inventory > Hardware > Detailed H	Hardware		14 Jul 2011, 12:34 UTC
Navigator	Inventory Hardware Report		
 Inventory Detailed Device 			
Device Attributes	Device Selector	Scheduling	
24-hour Inventory Change	< <search input="">> → 🗩</search>	Run Type: Immediate 💌	
 Hardware 	All Search Results Selection	Date: 14 3d 2011 at 12 - hh 40 - mm	
Chassis Slot Details	E C All Devices	Job Info	
Chassis Slot Summary	▼ \$3560-DC-1		
Chassis Summary Graph	3750-PHY-1	Job Description*:	
Detailed Hardware	1 3945-East-1	E-mail:	
Device Statistics		Attachment Option : Report type : PDF CSV	
Hardware Component Summary		Browse	
Hardware Summary Graph	2 device(s) selected		
Multi Service Port	Note: * - Required	Finish Reset	
EoS/EoL Hardware	The second		

- Select the devices that you want in the detailed hardware report.
- Choose the scheduling option. You can generate the report immediately or schedule it to be generated at the specified time.
 - If you choose to schedule it, specify the Job Info and click Finish. The finished report will appear under Reports->Report Archives->Inventory and Syslog.

If you choose Immediate as the scheduling option, the report (Figure 78) will be generated immediately.

Figure 78. The Detailed Hardware Report Specified in Figures 76 and 77

Europany				
Summary				
		Total number of devices:	2	
		Devices with Report Data:	2	
		Devices without Report Data:	None	
Category : S	witches and Hubs			
Cisco Cataly	st 3750 Series Swite	hes		
Device Name	Updated At	System Description		Locatio
3750-PHY-1	Jun 15 2011 10:55:3	Scisco IOS Software, C3750 Software (C3750-IPBASE-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Thu I	9-Jul-07 19:15 by nacher	nCampu
Cisco Cataly	st 3560-E Series Sw	itches		
Device Name	Updated At	System Description		
3560-DC-1	Jun 15 2011 10:55:03	Cisco IOS Software, C3560E Software (C3560E-UNIVERSAL-M), Version 12.2(52)SE, RELEASE SOFTWARE (fc3) Copyright (c) 1986-2009 by Cisco Systems, Inc. Compiled P	ri 25-Sep-09 02:04 by sa	asyamal
Back to Top	· · · · · · · · · · · · · · · · · · ·			

Work Centers

Cisco Prime LMS 4.1 provides complete lifecycle management of:

- Identity
- EnergyWise
- Medianet
- Auto Smartports
- Smart Install

LMS 4.1 provides a workflow-oriented approach for Day-1 to Day-**n** operations of Identity, EnergyWise, Medianet, Auto Smartports, and Smart Install (Figure 79). This workflow includes readiness assessment, configuration, monitoring, reporting, and troubleshooting.

Figure 79. Work Centers in Cisco Prime LMS 4.1

My Menu 🔻 Monitor 💌 1	nventory 🔻 Configuration 🔻	Reports 🔻	Admin 🔻	Work Centers 🔻			윤 🔂
Admin > Getting Started Getting Started with LMS CiscoWorks LAN Management administer Cisco networks. Ci infrastructure. New Features in LMS 4.1 P Improved Usability Identity Auto Smartports	Solution (LMS) provides you with scoWorks Getting Started helps EnergyWise Monitoring Smart Install	powerful featur you in setting	es that enab up LMS and	Identity Daribabard Getting Started Readness Assessment Configure Reports Jobs Go Smart Install Getting Started Readness Assessment Configure Reports Jobs Jobs	 EnergyWise Dashboard Getting Started Readness Assessment Configure • Settings • Reports • Jobs Medianet Dashboard Getting Started Readness Assessment Configure Reports Ibins 	Auto Smartports Getting Stated Readness Assessment Manage Templates Configure • Reports Jobs	011, 12:41 U
X Template Center	Local CiscoWorks Aut	horization Mode			> Advanced Configurations		

A detailed description of each of these workcenters will be discussed in a separate whitepaper.

Server Administration

This chapter deals with server administration to utilize optimally the resources of the server while also maintaining a current status of the network topology.
Log Rotation

One common problem in LMS server maintenance is to control the size of log files. Log rotation helps you manage the log files more efficiently. In previous versions, a command-line utility, logrot, is configured and run to rotate the log files. From LMS 3.1, logrot can be configured and scheduled to run on the GUI.

To configure log rotation, go to Admin→Log Rotation. See Figure 80.

Figure 80.	Configuring Log	Rotation

Admin > Sy	rstem > Log Rotation				
og Rota	ation				
og Rotation	n				
Log Rotat	tion Settings				
Backup Directory:		/var/adm/CSC0px/log	Browse		
Restart Da	emon Manager:				
Configure	Log files				
	-			1000 00S	Showing 1-54 of 54 records
	Name with location		Size (kb) 4	Format	No.of Backups
1. 💿	/var/adm/CSCOpx/log/Vnm	server.log	1000	gz	2
2. 🔘	/var/adm/CSCOpx/log/Vnm	collector.log	1000	gz	2
3. 🔘	/var/adm/CSCOpx/log/Vnmclient.log		1000	gz	2
4. 🔘	4. O /var/adm/CSCOpx/log/Vnmutils.log		1000	gz	2
5. 🔘	5. /var/adm/CSCOpx/log/DFMOGSServer.log		10000	gz	3
6. 🔘	6. O /var/adm/CSCOpx/log/DFMDeviceSelector.log		10000	gz	2
7. 🔘	/var/adm/CSCOpx/log/DFMLogServer.log		10000	gz	2
8. 🔘) /opt/CSCOpx/log/dfmLogs/TIS/TISServer.log		10000	gz	5
9. 🔘	/var/adm/CSCOpx/log/campusportal.log		1024	gz	2
10. 🔘	/var/adm/CSCOpx/log/netconfigclient.log		10240	gz	3
11. 🔘	/var/adm/CSCOpx/log/RME	Portlets.log	10240	gz	3

The backup directory stores the rotated log files. The default directory is:

- NMSROOT\log on Windows
- /var/adm/CSCOpx/log on Solaris and Soft Appliance

If you do not specify a backup directory, each log file will be rotated in its current directory.

You can also specify **Restart Daemon Manager** to stop and start the daemon before the log rotation starts. This is optional. To stop and start daemons in:

- Windows
 - net stop crmdmgtd
 - net start crmdmgtd
- Solaris or soft appliance
 - /etc/init.d/dmgtd stop
 - /etc/init.d/dmgtd start

To add the log files for rotation, click the **Add** button to add log files one by one.

Figure 81. Using Logrot to Specify Files for Log Rotation

Select Log File*:	Var/adm/CSCOpy/log Browse	
Maximum Logrot Size*:		
Compression Format:	NO 2	
No.of Backups:	0	

As shown in the Figure 81, you specify the log file name, maximum logrot size (the default is 1024KB, the maximum size is 4096MB), the compression format, and the number of backups. If you do not want to keep any archive, enter 0 for the number of backups.

Database Backup

You can backup the LMS database either through GUI or CLI. Before LMS 3.2, it is not possible to do selective backup/restore. The backup process backed up all configuration files from the application databases. In this release, you can back up the required system configurations and data from the command-line interface.

The following data is backed up when you run a backup from the user interface or from CLI:

- Cisco Primeuser information
- Single sign-on configuration
- DCR configuration
- · Peer certificates and self-signed certificates
- Peer server account information
- Login module settings
- Software Center map files
- · License data
- · Core client registry
- System identity account configuration
- · Cisco.com user configuration
- Proxy user configuration
- Database jobs and resources data, DCR data, groups data, and other data stored in the database
- · Discovery settings and scheduled jobs
- ACS credentials
- Local user policy setup
- System preferences

When you run a selective data backup from CLI, all the data mentioned above gets backed up except:

- Software Center map files
- Software Center jobs data

DCR jobs data

Backing Up Using CLI

To back up data using CLI on Windows, Solaris, and Linux:

• On Windows, run:

NMSROOT\bin\perl NMSROOT\bin\backup.pl<BackupDirectory><[LogFile]> [Num Generations]

On Solaris and Linux, run:

/opt/CSCOpx/bin/perl /opt/CSCOpx/bin/backup.pl<BackupDirectory><[LogFile]>
[Num Generations]

where:

BackupDirectory is the directory that you want to be your backup directory. This is mandatory. LogFile is the name of the log file that contains the details of the backup.

Num Generations is the maximum number of backup generations to be kept in the backup directory.

To back up only selective data using CLI on Windows and Solaris:

• On Windows, run:

```
NMSROOT\bin\perl NMSROOT\bin\backup.pl-dest=BackupDirectory {-system | -
history}[-log=LogFile] [-email=E-mail][-gen=Num Generations]
```

• On Solaris and Linux, run:

```
/opt/CSCOpx/bin/perl /opt/CSCOpx/bin/backup.pl-dest=BackupDirectory {-system|-
history} [-log=LogFile] [-email=E-mail] [-gen=Num_Generations]
```

where:

-dest=BackupDirectory is the directory where the backed up data to be stored. This is mandatory.

-system is the command-line option that allows you to back up only the selected system configurations from all applications instead of backing up the complete databases. This is mandatory.

-log=LogFile is the name of the log file that contains the details of the backup.

-gen=Num_Generations is the maximum number of backup generations to be retained in the backup directory.

Restoring Data on Solaris and Linux

To restore the data:

- 1. Log in as the superuser, and enter the root password.
- 2. Stop all processes by entering:

/etc/init.d/dmgtd stop

3. Restore the database by entering:

```
/opt/CSCOpx/bin/perl /opt/CSCOpx/bin/restorebackup.pl [-ttemporary directory] [-
gengenerationNumber] [-dbackup directory] [-h].
```

Where:

- [-ttemporary directory]: The restore framework uses a temporary directory to extract the content of the backup archive.
- By default the temporary directory is created under NMSROOT as NMSROOT/tempBackupData. You can customize this, by using this t option, where you can specify your own temp directory. This is to avoid overloading NMSROOT.
- [-gengenerationNumber]: Optional. By default, it is the latest generation. If generations 1 through 5 exist, then 5 will be the latest.
- [-dbackup directory]: Required. Which backup directory to use.
- [-h]: Provides help. When used with -d<backup directory> syntax, shows correct syntax along with available suites and generations.

To restore the most recent version, enter:

```
/opt/CSCOpx/bin/perl /opt/CSCOpx/bin/restorebackup.pl-dbackup directory
For example, -d /var/backup
```

- Examine the log file in the following location to verify that the database was restored by entering: /var/adm/CSCOpx/log/restorebackup.log
- 2. Restart the system:

/etc/init.d/dmgtd start

Restoring Data on Windows

To restore the data on Windows, make sure you have the correct permissions, and do the following:

1. Stop all processes by entering the following at the command line:

net stop crmdmgtd

2. Restore the database by entering:

```
NMSROOT\bin\perlNMSROOT\bin\restorebackup.pl [-ttemporary directory] [-gen generationNumber] [-dbackup directory] [-h]
```

where **MMSROOT** is the Cisco Prime LMSinstallation directory. See the previous section for command option descriptions.

To restore the most recent version, enter the following command:

NMSROOT\bin\perlNMSROOT\bin\restorebackup.pl-dbackup directory

- 3. Examine the log file in the following location to verify that the database was restored by entering: NMSROOT\log\restorebackup.log
- 4. Restart the system by entering:

net start crmdmgtd

While restoring using a backup taken from a machine that is in ACS mode, the machine on which data is restored needs to be added as a client in ACS. Contact the ACS administrator to add the restored machine as an ACS client. See also, Setting the Login Module to ACS, at the online help.

Cisco Smart Interactions

Cisco Prime LMS provides a new functionality called Cisco smart interactions to deliver personalized, automated self-help tools that speed the resolution of network problems, outages and trouble tickets. Cisco smart interactions are a key element of the Cisco smart services strategy to deliver actionable insight into the network through personalized, proactive capabilities. Cisco smart services bring Cisco industry knowledge, expertise, and tools to IT teams to help them predictably manage the health and stability of their networks.

Today, Cisco smart interactions for Cisco Prime for Enterprise products support two innovative features:

- Automated context-based help: This tool supports real-time access to the Cisco support community. It
 helps IT organizations reduce and in many cases eliminate the need to create TAC cases. It facilitates a
 context-relevant search across Cisco support communities, online documentation, and expert comments to
 automatically find the information most relevant to the problem.
- Automated Cisco Technical Assistance Center (TAC) case creation and management: This tool can
 automatically open, update and track a Cisco TAC case. This tool saves a significant amount of time for IT
 operators because all of the steps that they have taken to try to resolve the problem, including alarms,
 automated troubleshooting logs, and other contextual reference information from the management platform,
 can be included with the initial TAC case request. Cisco Smart Interaction can be accessed by hovering
 your mouse over any device name and using the device details pane (Figure 79).



Figure 82. Hover the Mouse over a Device Name for Details about the Device

Note that to open a TAC case, you need a valid Cisco.com username and password that LMS will prompt you to enter as you open the case. Also, make sure that your LMS server has Internet access to communicate with Cisco.com for authentication as well as for TAC database. See Figure 83.

Figure 83. Opening a TAC Case



Appendix A: List of Acronyms and Features

Acronym/Feature	Meaning
AAA	Authentication, authorization, and accounting.
ACS	Access Control Server, an AAA server software from Cisco.
Certificate Setup	This feature allows the creation of self-signed security certificates, which can be used to enable SSL connections between the client browser and management server.
CWHP	CiscoWorks homepage. A web page that a CiscoWorks user accesses after logging into a CiscoWorks server.
DCR	Device and Credentials Repository is a common repository of devices, their attributes, and the credentials required to manage devices in a management domain. DCR will enable the sharing of device information among various network management applications.
ELMI	Enhanced Local Management Interface. It is a protocol used in Metro Ethernet.
FR	Frame Relay.
ILMI	Integrated Local Management Interface. It is an ATM standard.
IOS	Internetwork Operating System. It is an operating system that runs Cisco routers and switches.
LMS	LAN Management Solution.
MISTP	Multiple Instances Spanning Tree Protocol. It is a Cisco proprietary standard.
MST	Multiple Spanning Tree Protocol. It is an IEEE standard derived from MISTP.
NDG	Network Device Group. A term used in ACS to group devices.
NMIM	Network Management Integration Module.
NMS	Network Management System.
NMSROOT	Installation of folder of LMS. On Windows the default is c:\program files\CSCOpx; on Solaris it is /opt/CSCOpx.
Peer Server Account Setup	This feature helps you create users who can programmatically login to CiscoWorks servers and perform certain tasks. These users should be set up to enable communication between multiple CiscoWorks servers.
Peer Server Certificate Setup	This feature allows you to add the certificate of another CiscoWorks server into a trusted store. This will allow one CiscoWorks server to talk to another, using SSL.
PVST	PerVLAN Spanning Tree Protocol.
RCP	Remote Copy Protocol.
IP SLA	Cisco IOS IP Service Level Agreement (SLA), a network performance measurement feature in Cisco IOS Software, provides a scalable, cost-effective solution for service-level monitoring. It eliminates the deployment of dedicated monitoring devices by including the "operation" capabilities in the routers.
SCP	Secure Copy Protocol.
Single Sign-On	A feature by which a single browser session is used to navigate transparently to multiple CiscoWorks servers without having to authenticate to each server.

Acronym/Feature	Meaning
SNMP	Simple Network Management Protocol.
SSH	Secure Shell Protocol.
SSL	Secure Sockets Layer. It is an encryption protocol.
SSO	Single sign-on: The ability to login to multiple computers or servers with a single action and the entry of a single password. Especially useful where, for example, a user on a LAN or WAN requires access to a number of different servers.
STP	Spanning Tree Protocol. A protocol to avoid loops in a switched network.
System Identity Setup	Communication between multiple Cisco Prime LMS servers is enabled by a trust model addressed by certificates and shared secrets. System Identity Setup should be used to create a "trust" user on slave/regular servers for communication to happen in multiserver scenarios.
TACACS+	Terminal Access Controller Access Control System Plus. It is an authentication protocol.
TLS	Transport Layer Security.
VLAN	Virtual local area network.
νтр	VLAN Trunk Protocol. A protocol used in a trunk link of two switches to maintain VLAN information in a switched network.



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA