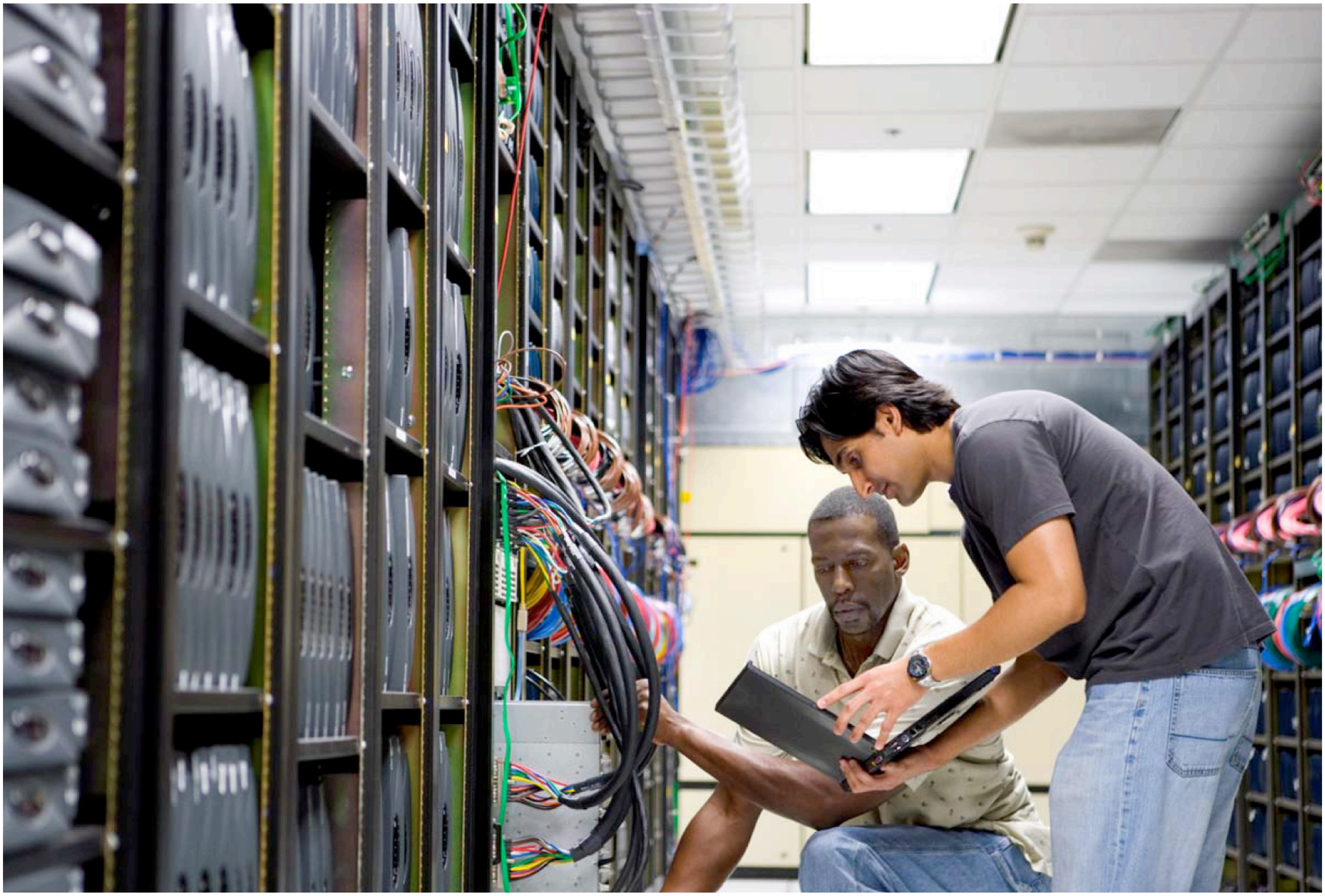
CiscoWorks LAN Management Solution 4.0

Deployment Guide



Contents

Cisco LMS 4.0 Deployment Guide

Introduction

CiscoWorks 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, CiscoWorks LMS allows network operators to manage a borderless network through a browser-based interface that can be accessed anytime from anywhere within the network.

CiscoWorks LAN Management Solution 4.0 provides significant improvements in usability, troubleshooting, and configuration management, simplifying end-to-end management of a Cisco borderless network, reducing operating expenses (OpEx), and improving network availability. Using the latest Web 2.0 technologies, the product provides a seamless, intuitive, task-based approach that simplifies the deployment of Cisco value-added services and technologies.

For detailed product information related to LMS, refer to the product portal at http://www.cisco.com/go/lms.

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/sw/cscowork/ps2425/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 4.0, 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/sw/cscowork/ps2425/prod_literature.html

Supported Device List (check out the Generic Device Support section in Chapter 7, Resource Manager Essentials [RME]): http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products_device_support_tables_list.html

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

Release Notes: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_release_notes_list.html

LMS Workflow

The steps below summarize LMS setup workflow, which covers the whole lifecycle of LMS server from initial setup to ongoing operations. The following chapters illustrate 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 CiscoWorks.

  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 4.0 guides you to do the initial setup through the **Getting Started** workflow from the **Admin** menu. This includes configuring basic server settings, automatically discovering the devices, or manually adding devices,

Setting up Devices on the Network

LAN Management Solution 4.0 helps in managing Cisco devices on the network. Before LMS 4.0 can function properly, the network devices that LMS interfaces with must be set up correctly in order to communicate with the CiscoWorks server. For example, the SNMP community strings must match between the device and the CiscoWorks 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 CiscoWorks LAN Management Solution. Keep in mind that this document is not intended to be a comprehensive configuration guide for LMS 4.0. 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 commands:

```
write memory
```

or

```
copy running-config startup-config
```

Please note that the above command is provided to save 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.

Generic Configuration of Devices

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 on the network, 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.

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#`**

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.

Table 1. Applications and Device Credentials

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
IP SLA 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

[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.

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 community string. The read-only 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

CiscoWorks can collect device configurations by either SNMP-write, which triggers Trivial File Transport Protocol (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 Campus Manager for configuration changes such as fixing discrepancies.

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 IOS Software

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

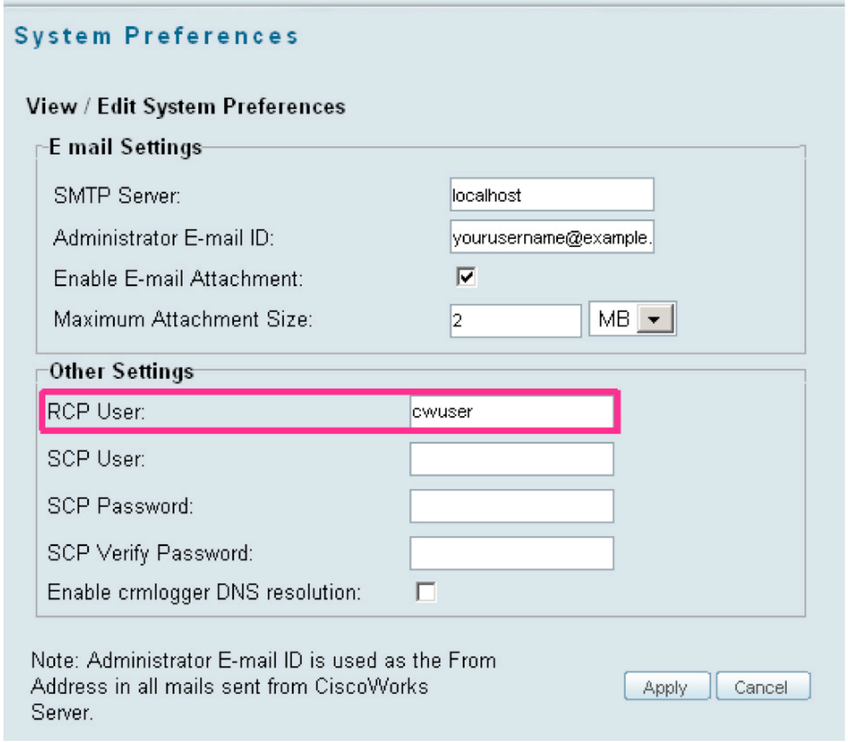
Remote Copy Protocol (RCP) is one of the protocols that can be used by LMS for configuration management and software image management. For LMS to be able to provide configuration and software management using RCP, it must be enabled on the devices.

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 RCP User 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 à System à System Preferences. See Figure 1.

Figure 1. System Preferences



System Preferences

View / 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:

Enable crmlogger DNS resolution: □

Note: Administrator E-mail ID is used as the From Address in all mails sent from CiscoWorks Server.

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.

Table 2. SCP Configuration

	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.
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: **username**name[**privilege**level]{**password**encryption-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:

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

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

To enable Cisco Discovery Protocol globally:

```
cdp run
```

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 by Campus Manager, 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.

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.

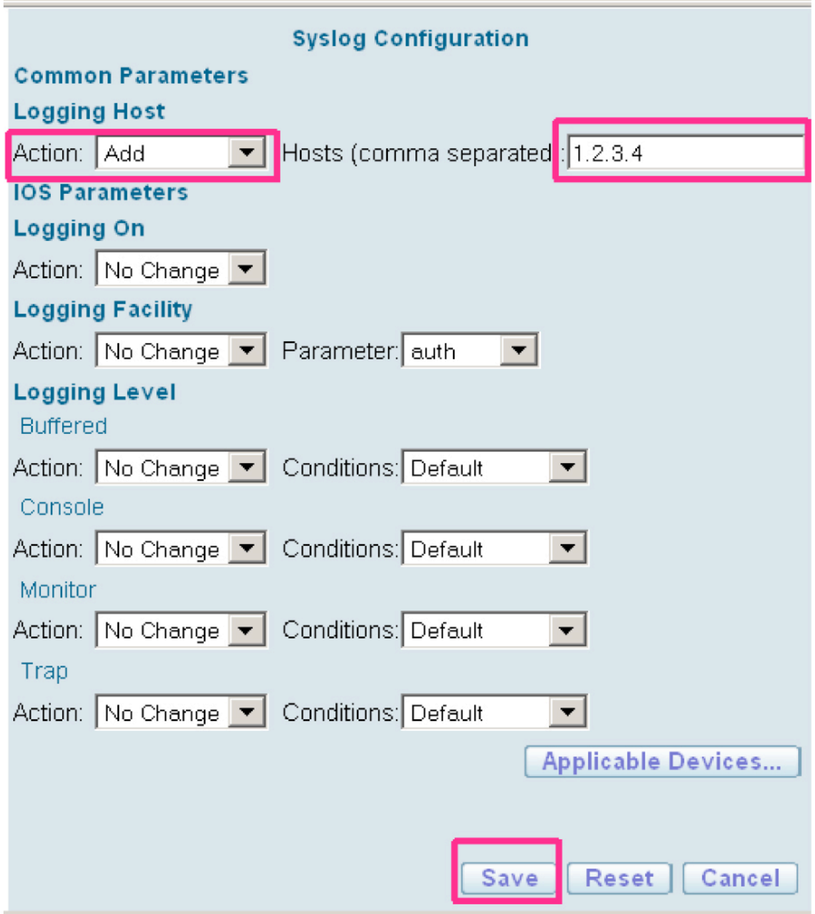
Syslog Messages

Syslog messages can be enabled on Cisco devices to fully use 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 on 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 on in this document (please refer to the section "*Create a NetConfig Job to Enable Syslogs on Devices and Configure LMS Server as Receiver*" in Chapter 5), but Figure 2 shows what an example syslog configuration will look like.

Figure 2. Turn on Syslog Using NetConfig



Syslog Configuration

Common Parameters

Logging Host

Action: Add ▼ Hosts (comma separated): 1.2.3.4

IOS Parameters

Logging On

Action: No Change ▼

Logging Facility

Action: No Change ▼ Parameter: auth ▼

Logging Level

Buffered

Action: No Change ▼ Conditions: Default ▼

Console

Action: No Change ▼ Conditions: Default ▼

Monitor

Action: No Change ▼ Conditions: Default ▼

Trap

Action: No Change ▼ Conditions: Default ▼

Protocol Setup on the LMS Server

Note: The settings described in this section will be finished after the LMS server is installed.

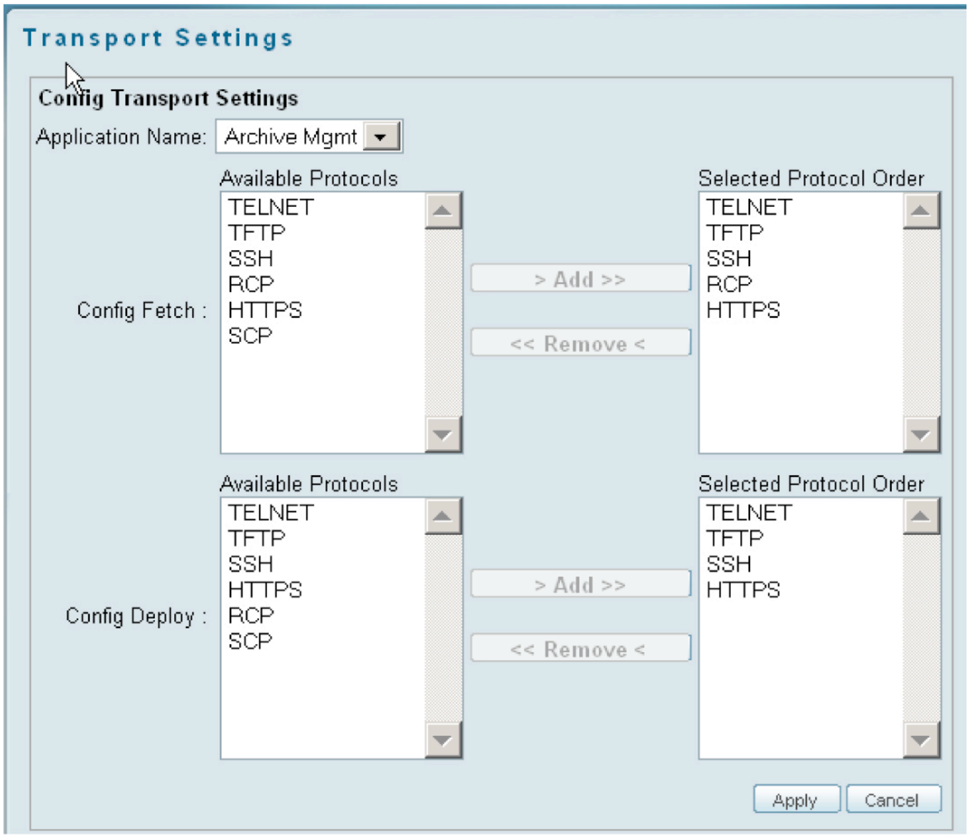
One of the most important areas of setup is LMS protocol setup. LMS uses various protocols for configuration and software management. Network administrators can assign the protocols to be used in LMS for configuration management and software management.

Configuration Management

You can set the protocols and order 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, SCP, and HTTPS.

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

Figure 3. Setting Up Protocol Ordering



Transport Settings

Config Transport Settings

Application Name: Archive Mgmt

Config Fetch :

Available Protocols: TELNET, TFTP, SSH, RCP, HTTPS, SCP

Selected Protocol Order: TELNET, TFTP, SSH, RCP, HTTPS

Config Deploy :

Available Protocols: TELNET, TFTP, SSH, HTTPS, RCP, SCP

Selected Protocol Order: TELNET, TFTP, SSH, HTTPS

As in Figure 3, for Config Fetch we use the SSH and TFTP protocols. LMS will first try SSH. If SSH does not work after three retries (not customizable) and timeouts (customizable, see below), LMS will fall back to TFTP, the next protocol on the list.

For secure communication between the server and device, use SSH.

Device Secondary Credentials

The LMS server polls and receives two types of credentials from each device and populates the repository. These credentials are:

- Primary credentials
- Secondary credentials

LMS uses either the primary or secondary credentials to access the devices using the following protocols:

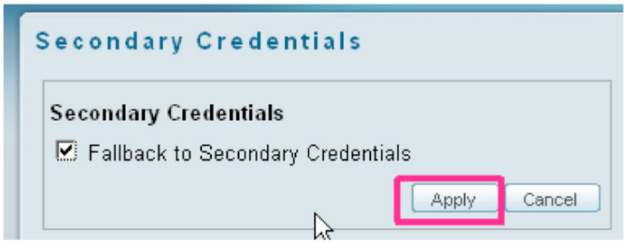
- Telnet
- SSH

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 4.

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

Admin settings: **Admin → Collection Settings → config → Secondary Credentials settings**

Figure 4. Device Secondary Credentials



Secondary Credentials

Secondary Credentials

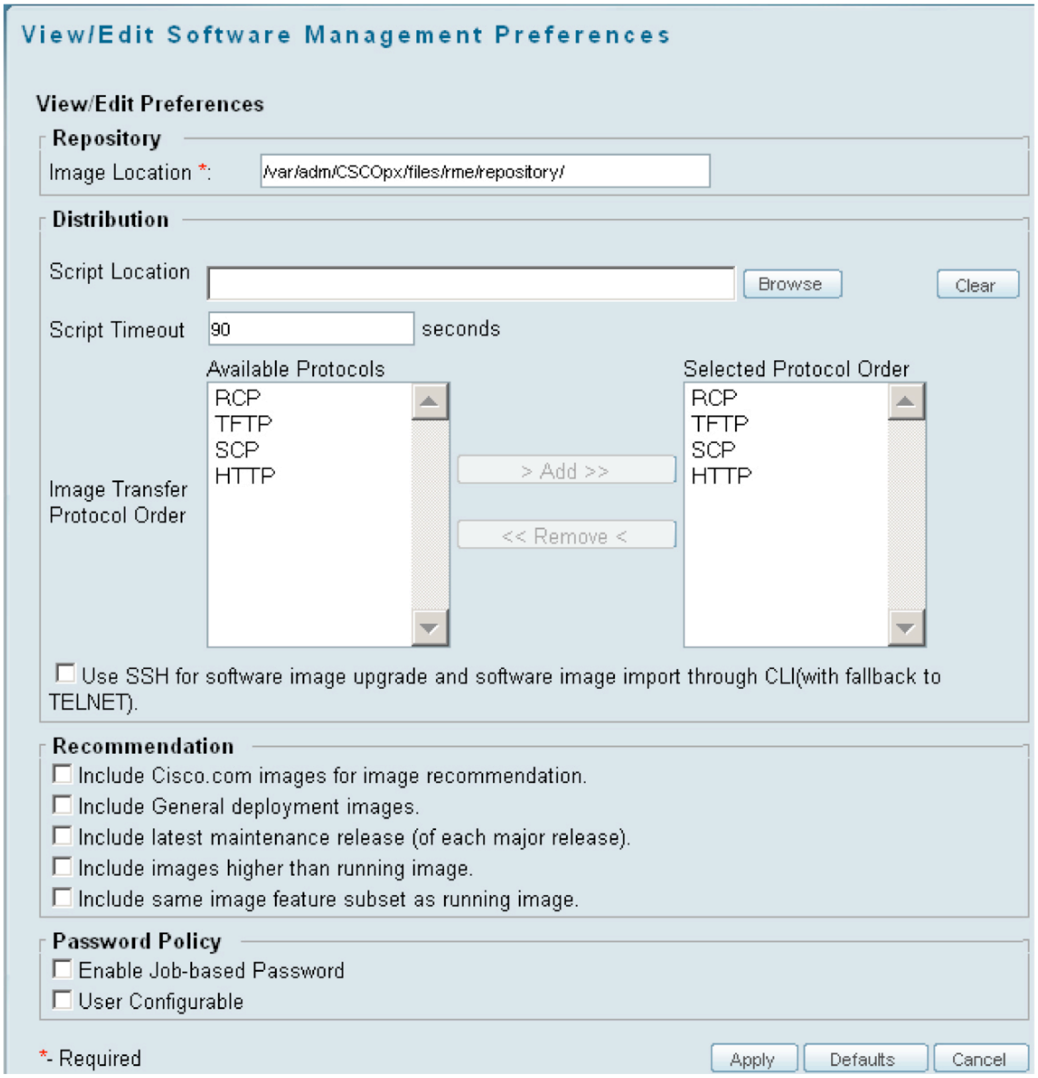
☑ Fallback to Secondary Credentials

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 5.

Figure 5. Software Image Management Options



View/Edit Software Management Preferences

View/Edit Preferences

Repository

Image Location *: /var/adm/CSCOpx/files/rme/repository/

Distribution

Script Location:

Script Timeout: 90 seconds

Image Transfer Protocol Order

Available Protocols: RCP, TFTP, SCP, HTTP

Selected Protocol Order: RCP, TFTP, SCP, HTTP

□ Use SSH for software image upgrade and software image import through CLI(with fallback to TELNET).

Recommendation

□ Include Cisco.com images for image recommendation.

□ Include General deployment images.

□ Include latest maintenance release (of each major release).

□ Include images higher than running image.

□ Include same image feature subset as running image.

Password Policy

□ Enable Job-based Password

□ User Configurable

*- Required

Cisco LAN Management Solution 4.0 Installation

Checklist Before Installation

Before starting the installation, we recommend that you:

- Make sure your server hardware and software meet the minimum requirements to install the LMS server. The requirements vary according to how many devices you want to manage, how many applications you are installing, how heavily you are using the applications, any need to use a virtual machine, and so on. Please refer to the installation guide "*Installing and Migrating to CiscoWorks LAN Management Solution 4.0*" at.
- Close all open or active programs. Do not run other programs during the installation process.
- While setting up the High Availability (HA) and Disaster Recovery (DR) environment in LMS server, be sure to set them prior to installing LMS.
- By default, SSL is not enabled on CiscoWorks Server.
- While launching CiscoWorks, network inconsistencies might cause installation errors if you are installing from a remote mount point.
- Disable any popup blocker utility that is installed on your client system before launching CiscoWorks.
- CiscoWorks LMS 4.0 is installed in the default directories:
    - On Solaris:/opt/CSCOpx
    - On Windows: *SystemDrive*:\Program Files\CSCOpx

  Where, *SystemDrive* is the Windows operating system installed directory.

  If you select another directory during installation, the application is installed in that directory.

  The destination folder should not contain the following special characters:

    - On Solaris:

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

      ! @ # $ % ^ & * ( ) + | } { " [ ] ; ' / ? < > , . ` =
- If errors occur during installation, check the installation log file:
    - On Solaris, check the installation log file /var/tmp/Ciscoworks_install_*YYYYMMDD_hhmmss*.log for LMS 4.0 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/Ciscoworks_install_20100721_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 4.0, the installation log file is:

      C:\Ciscoworks_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:\Ciscoworks_install_20100721_182205.log
- You can press **Ctrl-C** (on Solaris) 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.

- If HP OpenView is running on your system, installation will take more time. Disable HP OpenView to run a faster installation.
- To help ensure that you have the latest device support and bug fixes for LAN Management Solution you must install the latest Device Package updates.
- Enable 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.

We recommend that before installing the LMS 4.0 product, you register the product and receive a permanent license.

Licensing Process

The LMS 4.0 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.

Ordering Physical CiscoWorks LMS 4.0 DVD with Printed PAK

This is the traditional method of purchasing the product through Cisco direct and channel sales representatives. You will receive a kit with product DVDs and a software claim certificate paper, when you select this delivery method. The software claim certificate paper contains the PAK printed on it.

Downloading CiscoWorks LMS 4.0 Evaluation Software and Ordering Digital PAK

This option has been introduced to help ensure the faster delivery of the product. With this option, you can now:

- Download LMS 4.0 Evaluation software from http://www.cisco.com/go/nmsevals
- Order a digital PAK ID using the Cisco eDelivery application. After you have ordered the product in eDelivery and the electronic fulfillment is complete, you will receive the electronic software claim certificate with the digital PAK.

Available Licenses for LMS 4.0

Table 3 lists the available licenses and the permitted number of devices for traditional ordering.

Table 3. Traditional Ordering

Available Licenses (SKU) in LMS 4.0	Permitted number of Devices
CWLMS-4.0-SBE-K9 (Only for Windows)	50 Devices and 150 collectors
CWLMS-4.0-100-K9 (Only for Windows)	100 Devices and 300 collectors
CWLMS-4.0-300-K9	300 Devices and 1000 collectors
CWLMS-4.0-750-K9	750 Devices and 1250 collectors
CWLMS-4.0-1.5K-K9	1500 Devices and 1500 collectors
CWLMS-4.0-2.5K-K9	2500 Devices and 3000 collectors
CWLMS-4.0-5K-K9	5000 Devices and 5000 collectors
CWLMS-4.0-5K-K9	10,000 Devices and 5000 collectors

Licenses (SKUs) for LMS 4.0 Major Upgrade Kit

You need to order the upgrade licenses listed in Table 4 if you are upgrading from an earlier version of LMS.

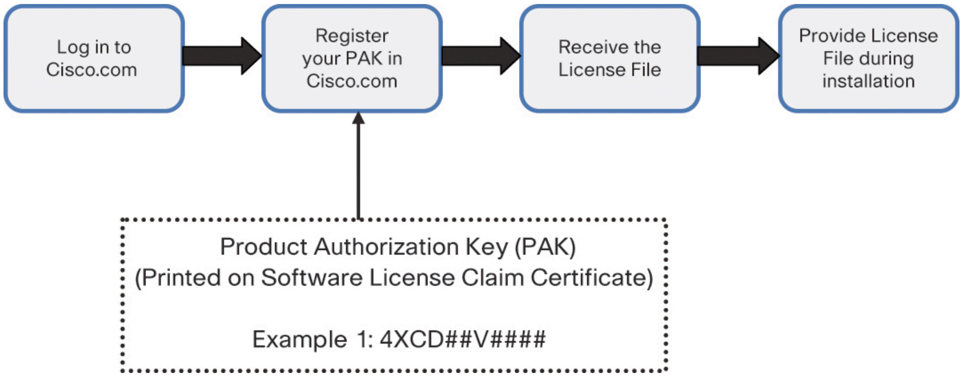
Table 4. Major Upgrade Kit

Licenses (SKU) to Upgrade from LMS 2.x or 3.x	Permitted number of Devices
CWLMS-4.0-100UPK9	LMS 4.0 100 Device Upgrade for LMS 2.x, 3.x users
CWLMS-4.0-300UPK9	LMS 4.0 300 Device Upgrade for LMS 2.x, 3.x users
CWLMS-4.0-1.5KUPK9	LMS 4.0 1500 Device Upgrade for LMS 2.x, 3.x users
CWLMS-4.0-5KUPK9	LMS 4.0 5000 Device Upgrade for LMS 2.x, 3.x users
CWLMS-4.0-10KUPK9	LMS 4.0 10,000 Device Upgrade for LMS 2.x, 3.x users

Steps to Follow for Licensing LMS

Figure 6 illustrates the steps for licensing LMS.

Figure 6. Steps for Licensing LMS


Log in to Cisco.com
Register your PAK in Cisco.com
Receive the License File
Provide License File during installation
Product Authorization Key (PAK)
(Printed on Software License Claim Certificate)
Example 1: 4XCD##V####

Step 1. Log on to 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 http://tools.cisco.com/RPF/register/register.do Once you get your Cisco.com user ID, log on to http://www.cisco.com/go/license o get your license file

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 4.0, 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 popup appears.

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

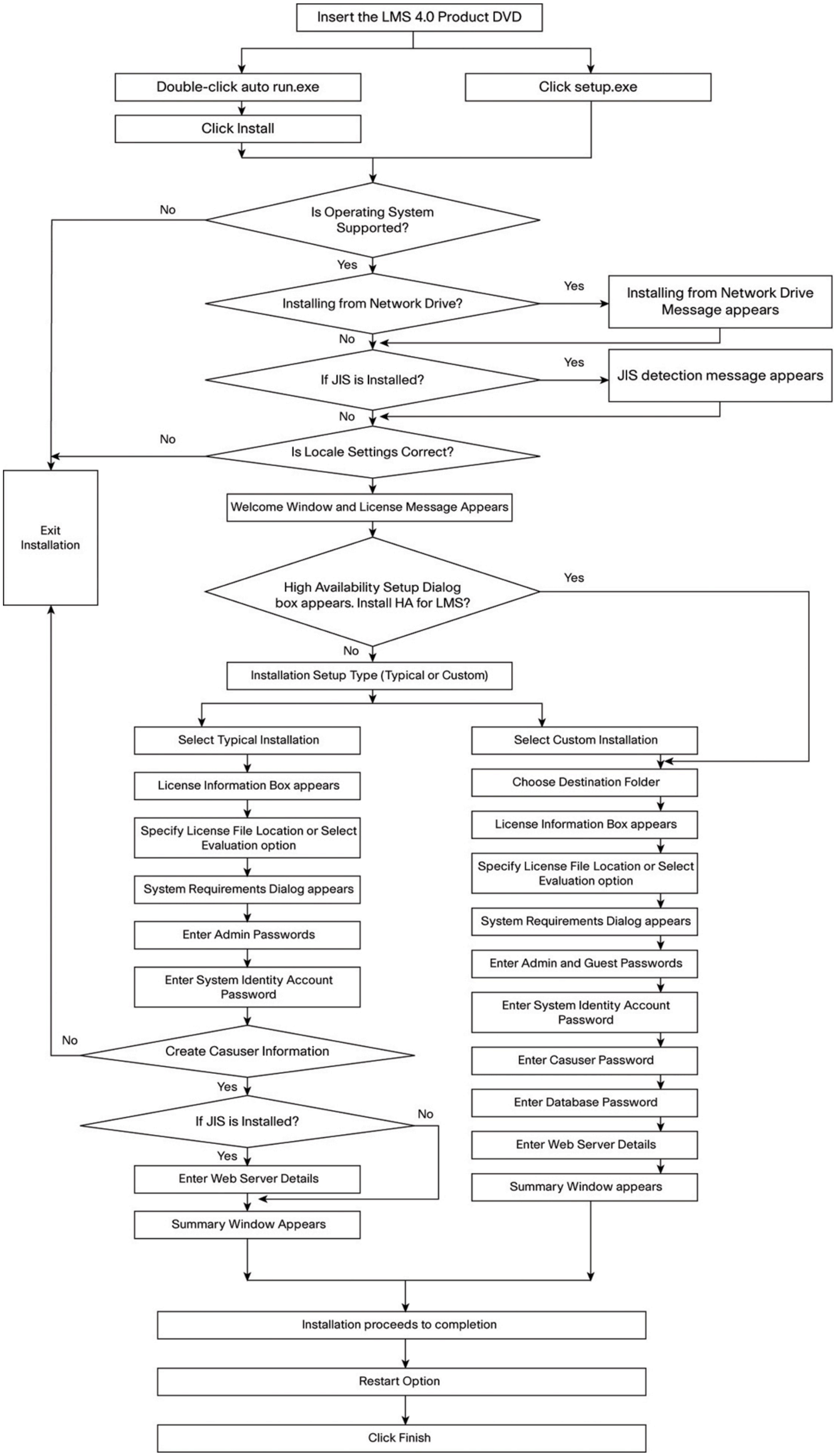
  The system verifies whether the license file is valid and updates the license.

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 4.0 on Windows

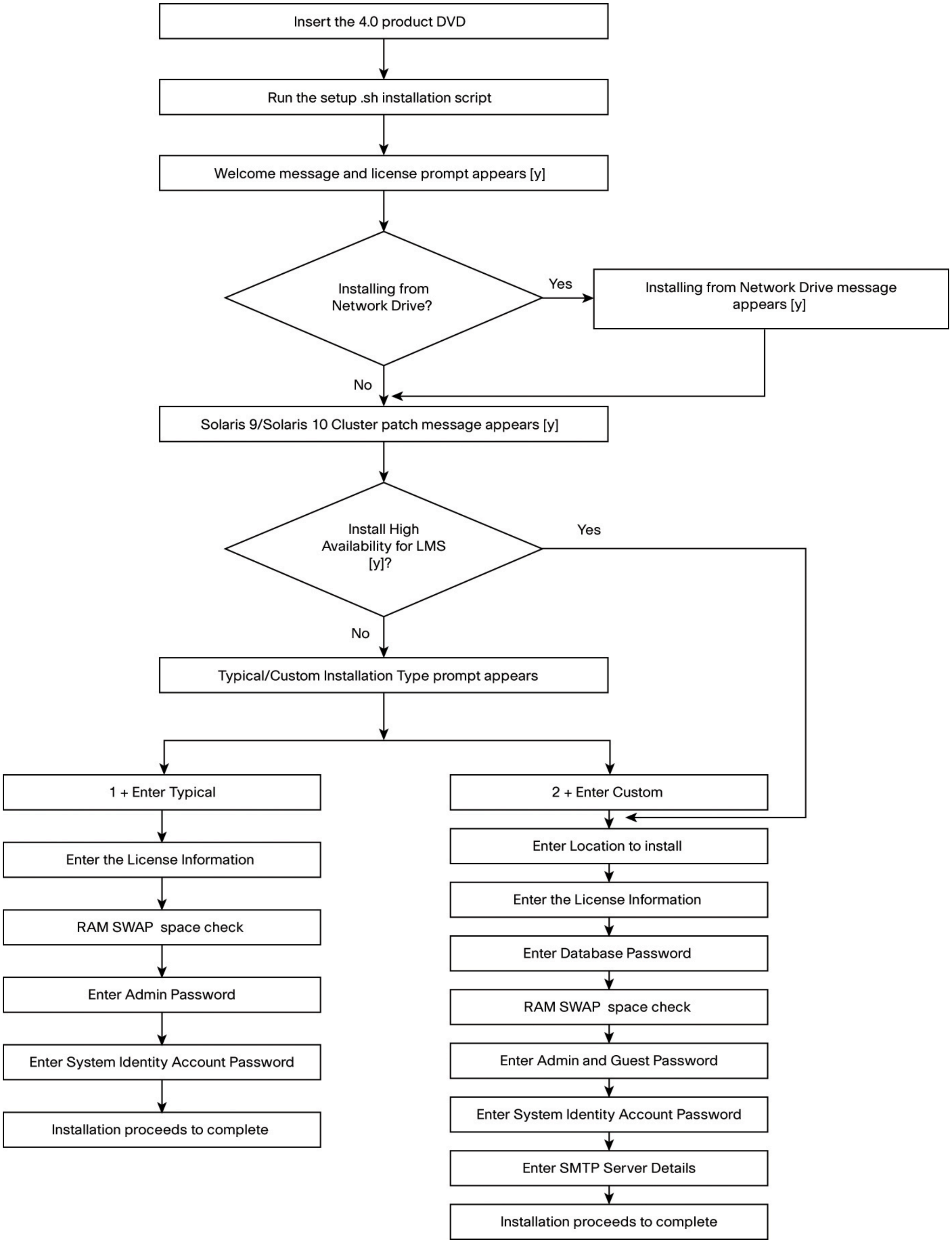
Thanks to the single-package installation design, the LMS installation programs on both Windows and Solaris are user friendly and fail-proof. See Figure 7 for a flow diagram of the installation procedure on Windows. See Figure 8 for a flow diagram of the installation procedure on Solaris.

Figure 7. Flow Diagram of Installation on Windows


Insert the LMS 4.0 Product DVD
Double-click auto run.exe
Click setup.exe
Click Install
Is Operating System Supported?
No
Yes
Installing from Network Drive?
Yes
Installing from Network Drive Message appears
No
If JIS is Installed?
Yes
JIS detection message appears
No
Is Locale Settings Correct?
No
Exit Installation
Welcome Window and License Message Appears
High Availability Setup Dialog box appears. Install HA for LMS?
Yes
No
Installation Setup Type (Typical or Custom)
Select Typical Installation
License Information Box appears
Specify License File Location or Select Evaluation option
System Requirements Dialog appears
Enter Admin Passwords
Enter System Identity Account Password
Create Casuser Information
No
Yes
If JIS is Installed?
No
Yes
Enter Web Server Details
Summary Window Appears
Select Custom Installation
Choose Destination Folder
License Information Box appears
Specify License File Location or Select Evaluation option
System Requirements Dialog appears
Enter Admin and Guest Passwords
Enter System Identity Account Password
Enter Casuser Password
Enter Database Password
Enter Web Server Details
Summary Window appears
Installation proceeds to completion
Restart Option
Click Finish

New Installation of LMS 4.0 on Solaris

Figure 8. Flow Diagram of Installation on Solaris


Insert the 4.0 product DVD
Run the setup .sh installation script
Welcome message and license prompt appears [y]
Installing from Network Drive?
Yes
Installing from Network Drive message appears [y]
No
Solaris 9/Solaris 10 Cluster patch message appears [y]
Install High Availability for LMS [y]?
Yes
No
Typical/Custom Installation Type prompt appears
1 + Enter Typical
Enter the License Information
RAM SWAP space check
Enter Admin Password
Enter System Identity Account Password
Installation proceeds to complete
2 + Enter Custom
Enter Location to install
Enter the License Information
Enter Database Password
RAM SWAP space check
Enter Admin and Guest Password
Enter System Identity Account Password
Enter SMTP Server Details
Installation proceeds to complete

Verifying the LMS 4.0 Installation

After you install CiscoWorks LMS 4.0 on Windows, you must verify the installation. To do this:

- Launch CiscoWorks: http://server_name:1741

  where server_name is the name of the CiscoWorks server and 1741 is the TCP port used by the CiscoWorks server.

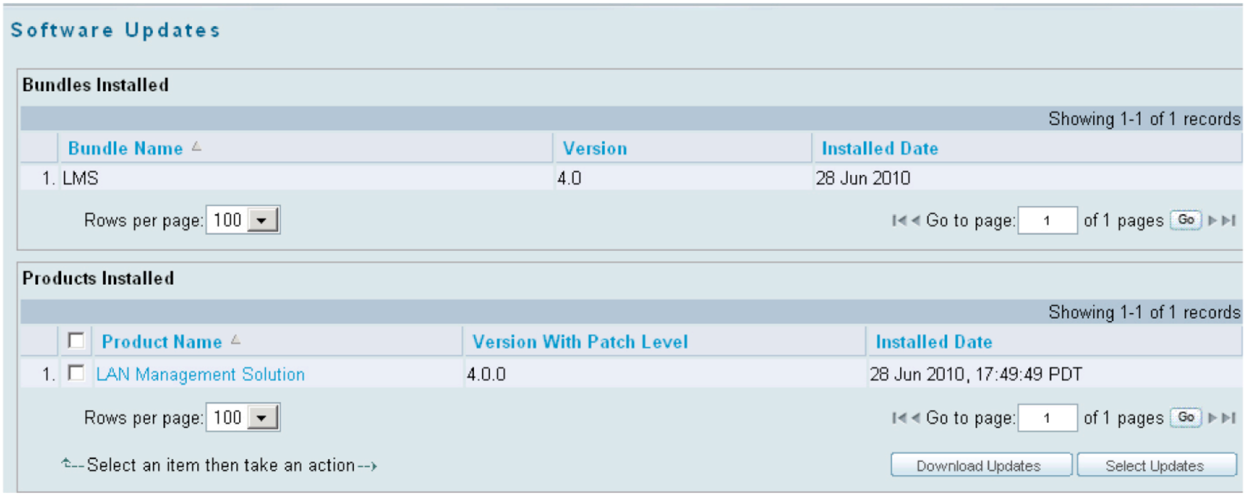
  In normal mode (HTTP), the default TCP port for the CiscoWorks server is 1741. When SSL (HHTPS) is enabled, the default TCP port for the CiscoWorks server is 443.

  You can change the HTTPS port number of the CiscoWorks server during the installation.

- Select **Admin → System → Software Center → Software Update**.

The Software Updates window appears (Figure 9).

Figure 9. The Software Updates Window



Software Updates

Bundles Installed

Showing 1-1 of 1 records

	Bundle Name	Version	Installed Date
1.	LMS	4.0	28 Jun 2010

Rows per page: 100

Go to page: 1 of 1 pages

Products Installed

Showing 1-1 of 1 records

	□	Product Name	Version With Patch Level	Installed Date
1.	□	LAN Management Solution	4.0.0	28 Jun 2010, 17:49:49 PDT

Rows per page: 100

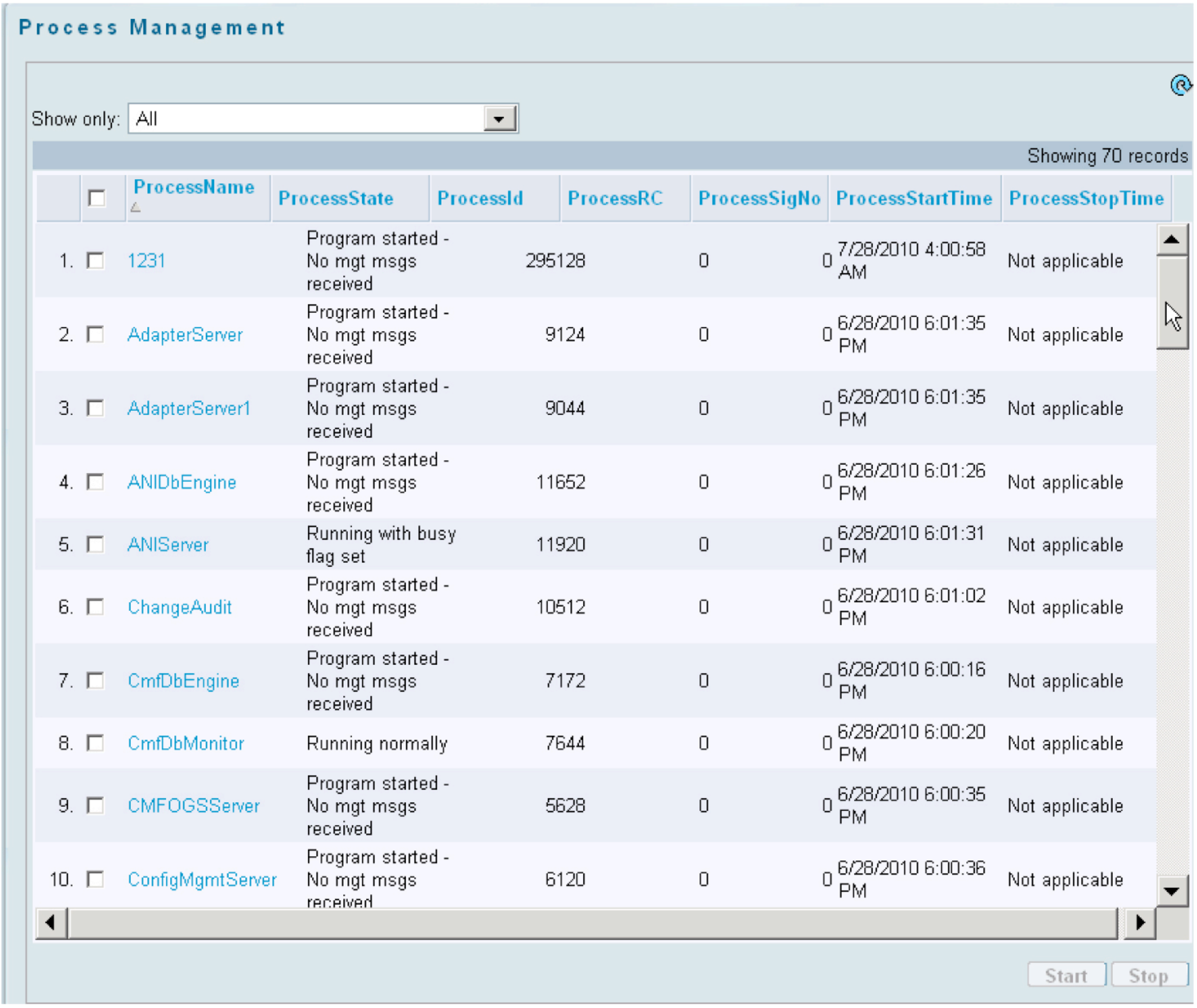
Go to page: 1 of 1 pages

Select an item then take an action-->

or

- Select **Admin → System → Server Monitoring → Processes** to see various process statuses (Figure 10).

Figure 10. The Process Management Window



Show only: All

Showing 70 records

	□	ProcessName	ProcessState	ProcessId	ProcessRC	ProcessSigNo	ProcessStartTime	ProcessStopTime
1.	□	1231	Program started - No mgt msgs received	295128	0	0	7/28/2010 4:00:58 AM	Not applicable
2.	□	AdapterServer	Program started - No mgt msgs received	9124	0	0	6/28/2010 6:01:35 PM	Not applicable
3.	□	AdapterServer1	Program started - No mgt msgs received	9044	0	0	6/28/2010 6:01:35 PM	Not applicable
4.	□	ANIDbEngine	Program started - No mgt msgs received	11652	0	0	6/28/2010 6:01:26 PM	Not applicable
5.	□	ANIServer	Running with busy flag set	11920	0	0	6/28/2010 6:01:31 PM	Not applicable
6.	□	ChangeAudit	Program started - No mgt msgs received	10512	0	0	6/28/2010 6:01:02 PM	Not applicable
7.	□	CmfDbEngine	Program started - No mgt msgs received	7172	0	0	6/28/2010 6:00:16 PM	Not applicable
8.	□	CmfDbMonitor	Running normally	7644	0	0	6/28/2010 6:00:20 PM	Not applicable
9.	□	CMFOGSServer	Program started - No mgt msgs received	5628	0	0	6/28/2010 6:00:35 PM	Not applicable
10.	□	ConfigMgmtServer	Program started - No mgt msgs received	6120	0	0	6/28/2010 6:00:36 PM	Not applicable

Ports Used by LMS Applications

Make sure the ports listed in Table 5 are open on the CiscoWorks server, or are not used by other applications.

Table 5. LMS Application Port Usage

Protocol	Port Number	Service Name	Applications	Direction (of Establishment) of Connection
TCP	49	TACACS+ and Access Control Server (ACS)	Common Services, Configuration and Software Image Management, Topology and Identity Services, Fault Management, IP SLA Monitoring	Server to ACS
TCP	25	Simple Mail Transfer Protocol (SMTP)	CiscoWorks Common Services (PSU), Inventory, Configuration and Image Management	Server to SMTP server
TCP	22	SSH	Common Services, Topology and Identity Services, Inventory, Config and Image Management	Server to device
TCP	23	Telnet	Common Services, Topology and Identity Services, Inventory, Config and Image Management	Server to device
User Datagram Protocol (UDP)	69	TFTP	Common Services, Inventory, Config and Image Management	Server to device Device to server

Protocol	Port Number	Service Name	Applications	Direction (of Establishment) of Connection
UDP	161	SNMP	Common Services, CiscoView, Inventory, Config and Image Management, Topology and Identity Services, Fault Management, IP SLA Performance Management, and Device Performance Management	Server to device Device to server
TCP	514	Remote Copy Protocol	Common Services	Server to device
UDP	162	SNMP traps (standard port)	Topology and Identity Services and Fault management	Device to server
UDP	514	Syslog	Common Services, Inventory, Config 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
TCP	443	CiscoWorks HTTP server in SSL mode	CiscoWorks Common Services	Client to server Server internal
TCP	1741	CiscoWorks HTTP Protocol	CiscoWorks Common Services, CiscoView, Topology and Identity Services, Inventory, Config and Image Management, Fault Management, and Internetwork Performance Monitor (IPM)	Client to server
UDP	42342	OSAGENT	Common Services	Client to server (for ANIServer)
TCP	42352	ESS HTTP (alternate port is 44352/tcp)	Common Services	Client to server
TCP	8898	Log server	Fault Management	Server internal
TCP	9002	DynamID authentication (Device Fault Manager [DFM] broker)	Fault Management	Server internal
TCP	9007	Tomcat shutdown	Common Services	Server internal
TCP	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
TCP	15000	Log server	Fault Management	Server internal
TCP	40050-40070	CSTM ports used by CS applications, such as OGS, DCR	Common Services	Server internal
TCP	40401	LicenseServer	Common Services	Server internal
TCP	43242	ANIServer	Topology and Identity Services	Server internal
TCP	42340	CiscoWorks Daemon Manager-Tool for Server Processes	Common Services	Server internal
TCP	42344	ANI HTTP server	Common Services	Server internal
UDP	42350	Event Services Software (ESS) (alternate port is 44350/udp)	Common Services	Server internal
TCP	42351	Event Services Software (ESS) listening (alternate port is 44351/tcp)	Common Services	Server internal
TCP	42353	ESS routing (alternate port is 44352/tcp)	Common Services	Server internal
TCP	43441	Common Services database	Common Services	Server internal
TCP	43455	Inventory, Config and Image Management Database	Inventory, Config and Image Management	Server internal
TCP	43443	ANIDbEngine	Topology and Identity Services	Server internal
TCP	43445	Fault history database	Fault Management	Server internal

Protocol	Port Number	Service Name	Applications	Direction (of Establishment) of Connection
TCP	43446	Inventory service database	Fault Management	Server internal
TCP	43447	Event Promulgation Module database	Fault Management	Server internal
TCP	44400-44420	CSTM ports	Fault Management, Device Performance Management	Server internal
TCP	47000-47040	CSTM port	Inventory, Config and Image Management	Server internal
TCP	49154	UPMDbEngine	Device Performance Management	Server internal
TCP	49155	OpsxmlDbEngine, JDBC/ODBC	CiscoWorks Assistant	Server internal
TCP	49157	IPSLA Performance Management Database	IPSLA Management	Server internal
TCP	50001	SOAPMonitor	Inventory, Config and Image Management	Server internal
TCP	55000-55020	CSTM port for Topology and Identity Services	Topology and Identity Services	Server internal

Getting started with LMS 4.0

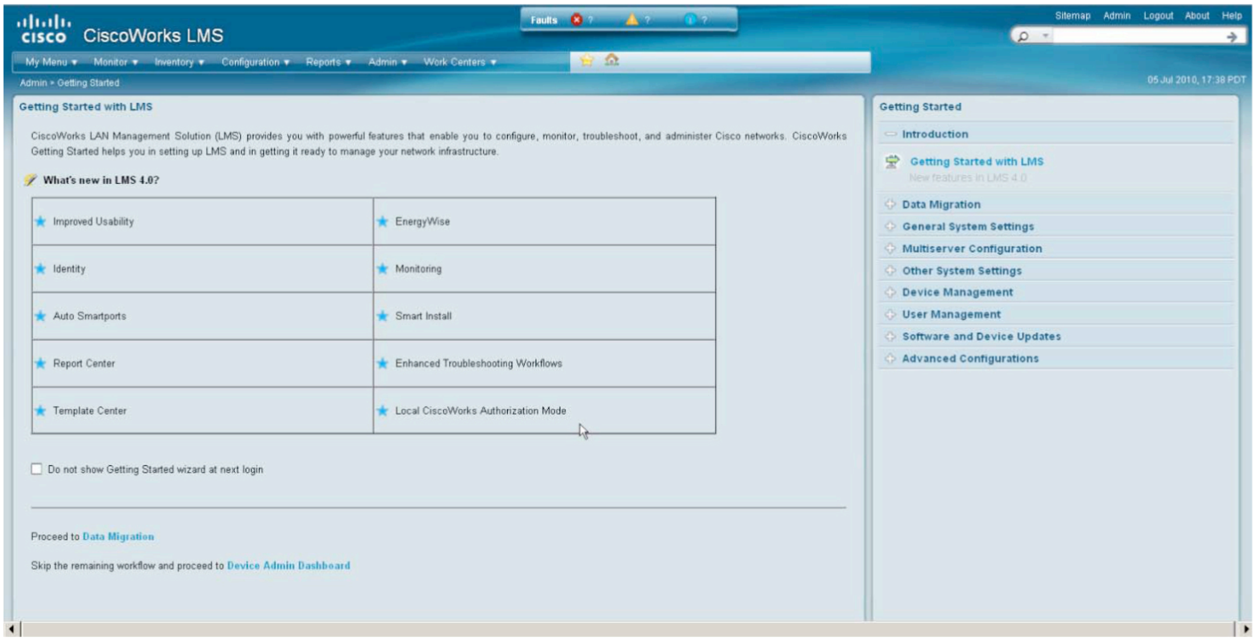
The LMS Getting Started workflow assists you in performing the tasks required to get your CiscoWorks LMS ready and to manage your Cisco networks.

When you log in to CiscoWorks LMS server for the first time, the Introduction page of the Getting Started workflow appears. The Introduction page lists the new features added in CiscoWorks LMS 4.0. 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
- Links to advanced functionalities and settings

You can configure these tasks step-by-step using the Getting Started workflow. You can also execute these tasks independently by selecting the task from the Getting Started assistant pane (Figure 11).

Figure 11. The Getting Started Assistant Pane



Getting Started with LMS

CiscoWorks LAN Management Solution (LMS) provides you with powerful features that enable you to configure, monitor, troubleshoot, and administer Cisco networks. CiscoWorks Getting Started helps you in setting up LMS and in getting it ready to manage your network infrastructure.

What's new in LMS 4.0?

Improved Usability	EnergyWise
Identity	Monitoring
Auto Smartports	Smart Install
Report Center	Enhanced Troubleshooting Workflows
Template Center	Local CiscoWorks Authorization Mode

□ Do not show Getting Started wizard at next login

Proceed to Data Migration

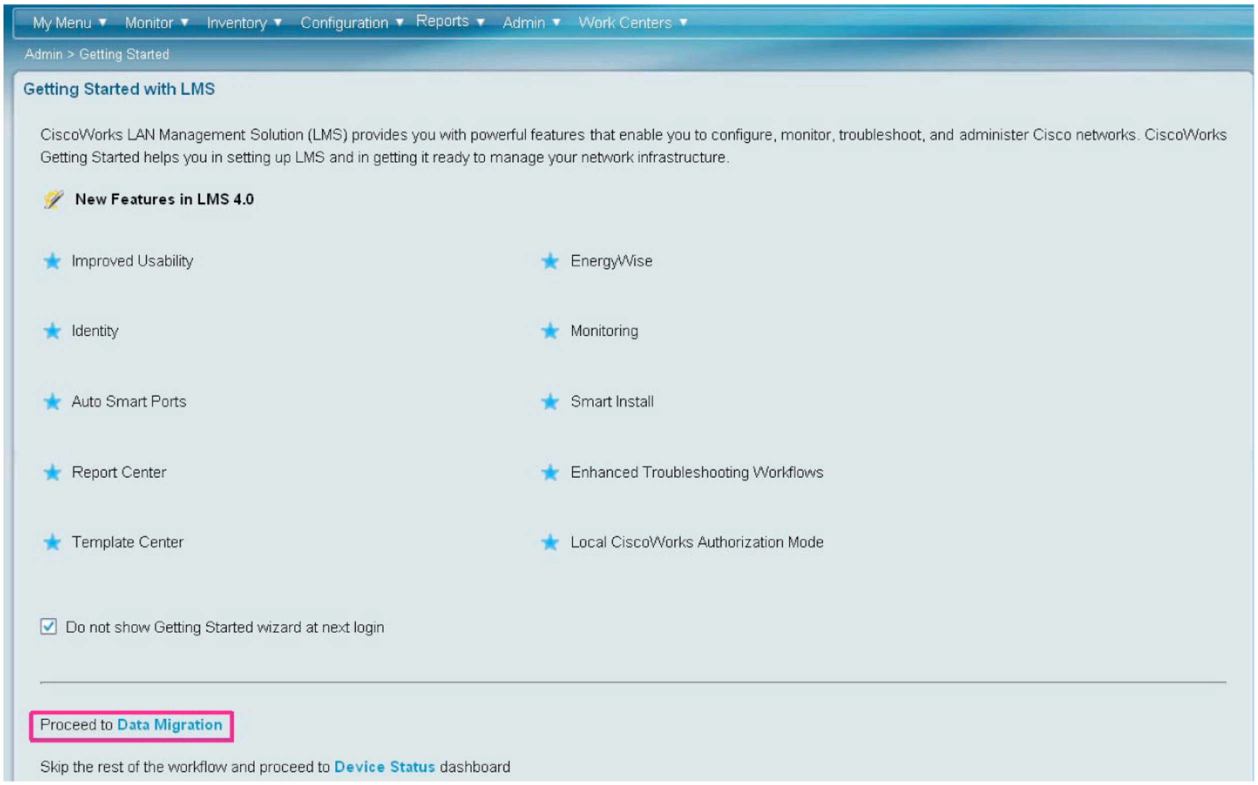
Skip the remaining workflow and proceed to Device Admin Dashboard

Getting Started

- Introduction
- Getting Started with LMS
  New features in LMS 4.0
- Data Migration
- General System Settings
- Multiserver Configuration
- Other System Settings
- Device Management
- User Management
- Software and Device Updates
- Advanced Configurations

You can follow the workflow by clicking the Proceed to Data Migration link (Figure 12) or, if you know the next step, you can click on any of the steps on the right hand side.

Figure 12. The Proceed to Data Migration Link



Getting Started with LMS

CiscoWorks LAN Management Solution (LMS) provides you with powerful features that enable you to configure, monitor, troubleshoot, and administer Cisco networks. CiscoWorks Getting Started helps you in setting up LMS and in getting it ready to manage your network infrastructure.

New Features in LMS 4.0

Improved Usability	EnergyWise
Identity	Monitoring
Auto Smart Ports	Smart Install
Report Center	Enhanced Troubleshooting Workflows
Template Center	Local CiscoWorks Authorization Mode

☑ Do not show Getting Started wizard at next login

Proceed to Data Migration

Skip the rest of the workflow and proceed to Device Status dashboard

Data Migration

This section describes how you can do the data migration from the previous version of LMS to LMS 4.0. It is assumed that you have backed up your current LMS installation.

Important: You have to freshly install LMS 4.0 on a new server and then perform data migration from the previous version of LMS that was backed up. The migration path is available for the following versions of LMS:

- LMS 3.2
- LMS 3.1
- LMS 3.0 Dec 2007 Update
- LMS 2.6

To start data migration:

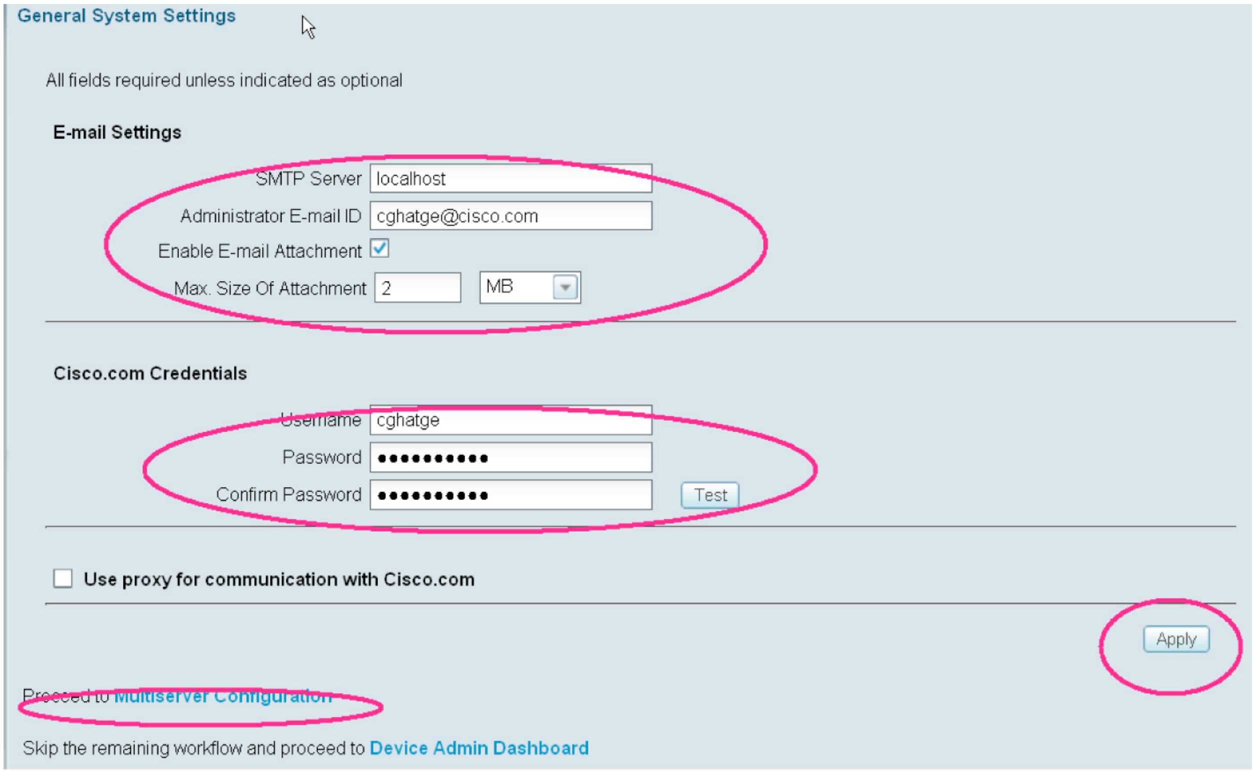
1. Store the backup archive in the server to which you want to migrate the data.
2. Go to the command prompt and stop the daemons using the following command:
    - For Windows:
      net stop crmdmgtd
    - For Solaris:
      /etc/init.d/dmgtd stop
3. Run the command:
    - For Windows:
      NMSROOT\bin\perl 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 CiscoWorks 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

Click the Proceed to **General System Settings** link for the next steps (see Figure 13).

General System Settings

Figure 13. General System Settings Showing Email Settings and Credentials



General System Settings

All fields required unless indicated as optional

E-mail Settings

SMTP Server: localhost

Administrator E-mail ID: cghatge@cisco.com

Enable E-mail Attachment: ☑

Max. Size Of Attachment: 2 MB

Cisco.com Credentials

Username: cghatge

Password: ●●●●●●●●●●

Confirm Password: ●●●●●●●●●●

□ Use proxy for communication with Cisco.com

Proceed to Multiserver Configuration

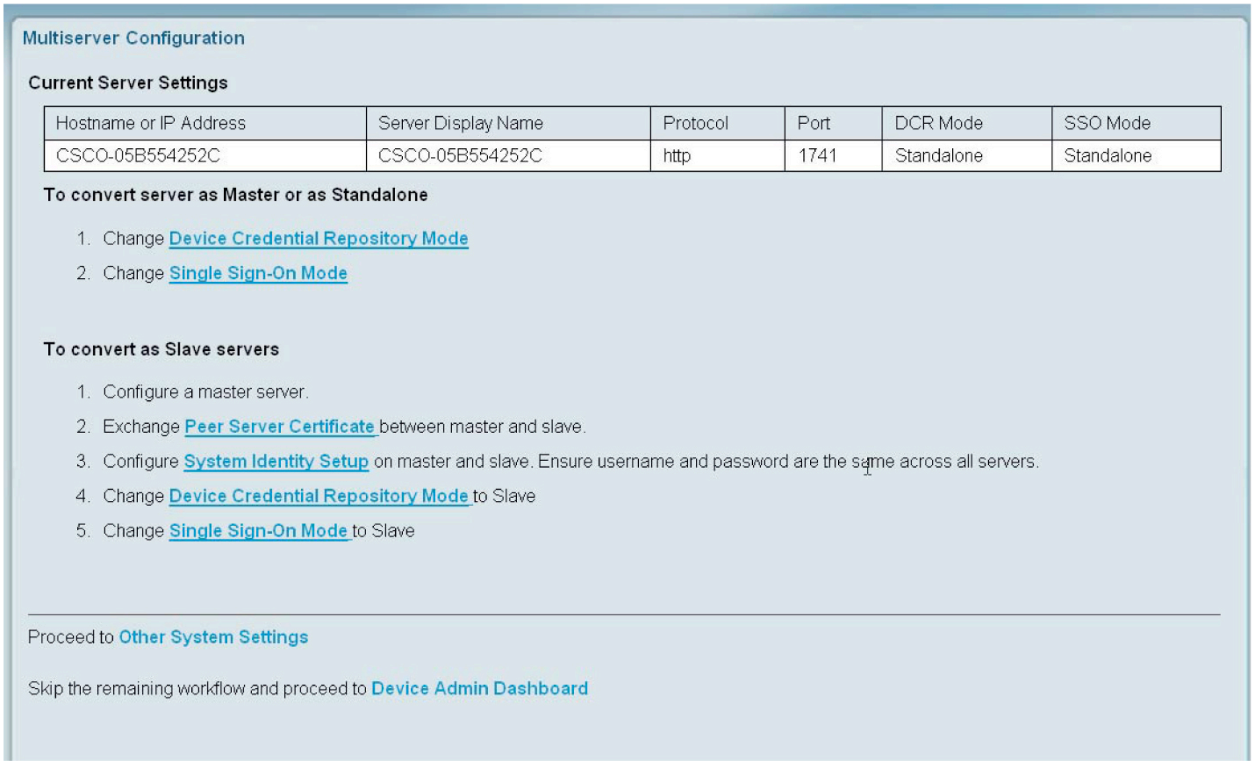
Skip the remaining workflow and proceed to Device Admin Dashboard

- Customization: You can personalize the CiscoWorks homepage using the drag-and-drop, add, edit, and remove features.
- Information available zero-click: Easy and quick access to the frequently viewed vital information pulled directly from the applications in the CiscoWorks LMS suite
- Multiserver support: Lists all of the portlets based on the applications installed on remote servers
- Lightweight GUI: Eliminates the need to install any plug-ins to launch the application

Multiserver Configuration

For advanced users, CiscoWorks LMS Setup Center is a centralized area where the user can quickly complete the CiscoWorks system configurations. One of the most common observations from new CiscoWorks users is that it is difficult to remember which application menu to navigate to when changing a system setting. CiscoWorks LMS Setup Center was designed to provide shortcuts to those options that may be difficult to find. It allows you to configure the necessary server settings immediately after installing the CiscoWorks LMS software. The Edit icon displayed for each setting takes you to the respective application page to configure the settings. See Figure 14.

Figure 14. Multiserver Configuration



Multiserver Configuration

Current Server Settings

Hostname or IP Address	Server Display Name	Protocol	Port	DCR Mode	SSO Mode
CSCO-05B554252C	CSCO-05B554252C	http	1741	Standalone	Standalone

To convert server as Master or as Standalone

1. Change Device Credential Repository Mode
2. Change Single Sign-On Mode

To convert as Slave servers

1. Configure a master server.
2. Exchange Peer Server Certificate between master and slave.
3. Configure System Identity Setup on master and slave. Ensure username and password are the same across all servers.
4. Change Device Credential Repository Mode to Slave
5. Change Single Sign-On Mode to Slave

Proceed to Other System Settings

Skip the remaining workflow and proceed to Device Admin Dashboard

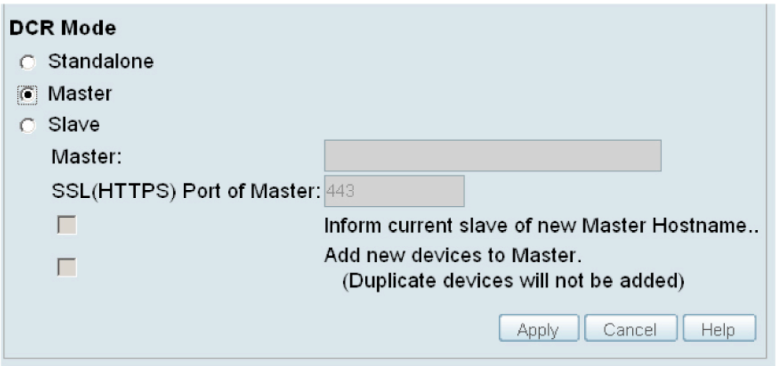
The most common installations are stand-alone single-server. If you are doing the multiserver deployment, then you can skip this section and click Proceed to **Other System Settings**.

Designate This Server as Master

1. **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**. See Figure 15.

Figure 15. Changing the DCR Mode to Master



DCR Mode

○ Standalone

● Master

○ Slave

Master:

SSL(HTTPS) Port of Master: 443

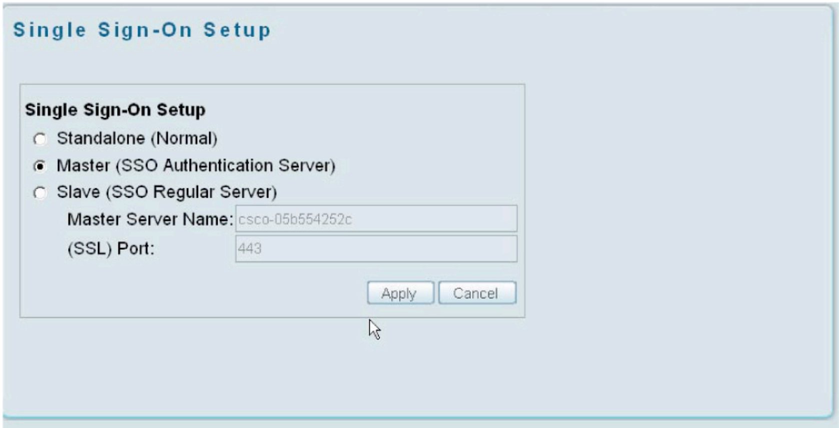
□ Inform current slave of new Master Hostname..

□ Add new devices to Master.
(Duplicate devices will not be added)

2. **Change Single Sign-On mode**

   Choose **Master** and click **Apply**. See Figure 16.

Figure 16. Changing Single Sign-On Mode



Single Sign-On Setup

Single Sign-On Setup

○ Standalone (Normal)

● Master (SSO Authentication Server)

○ Slave (SSO Regular Server)

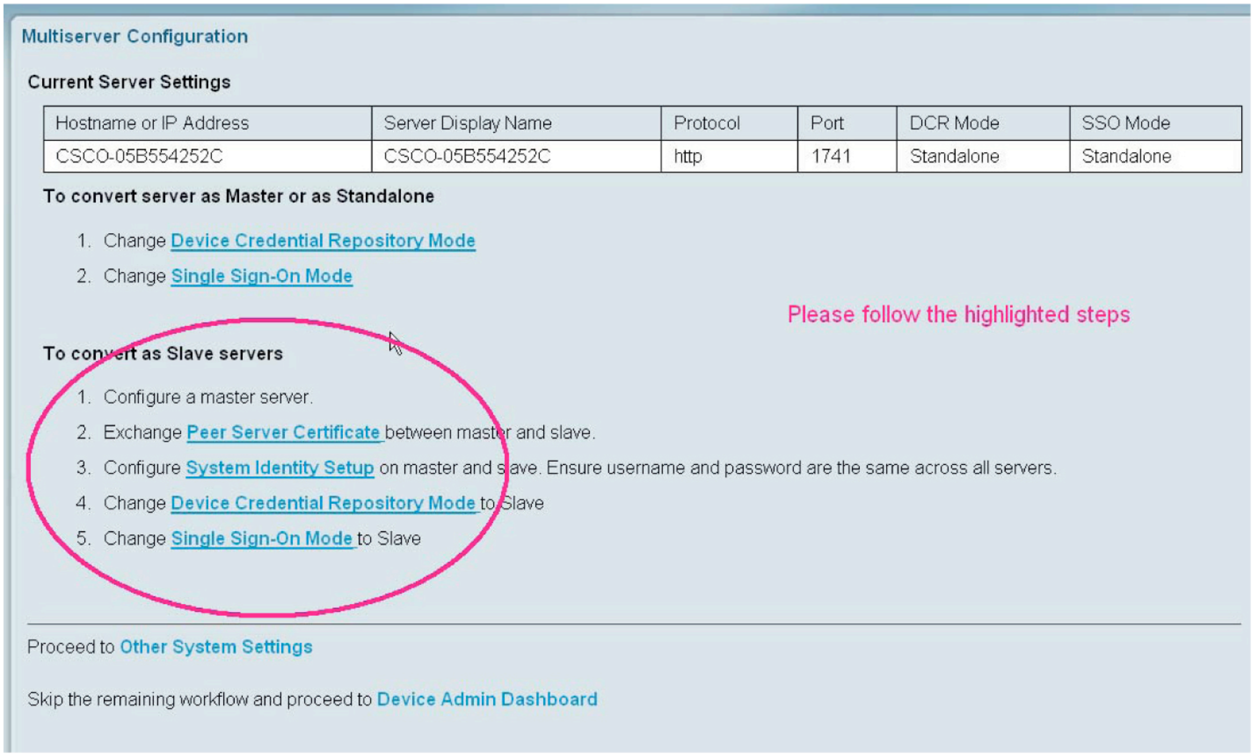
Master Server Name: csco-05b554252c

(SSL) Port: 443

Designate This Server as Slave

Figure 17 illustrates the steps to configure the server(s) as slave.

Figure 17. Configuring the Server as Slave



Multiserver Configuration

Current Server Settings

Hostname or IP Address	Server Display Name	Protocol	Port	DCR Mode	SSO Mode
CSCO-05B554252C	CSCO-05B554252C	http	1741	Standalone	Standalone

To convert server as Master or as Standalone

1. Change Device Credential Repository Mode
2. Change Single Sign-On Mode

Please follow the highlighted steps

To convert as Slave servers

1. Configure a master server.
2. Exchange Peer Server Certificate between master and slave.
3. Configure System Identity Setup on master and slave. Ensure username and password are the same across all servers.
4. Change Device Credential Repository Mode to Slave
5. Change Single Sign-On Mode to Slave

Proceed to Other System Settings

Skip the remaining workflow and proceed to Device Admin Dashboard

Click the Proceed to **Other System Settings** link to continue.

Other System Settings

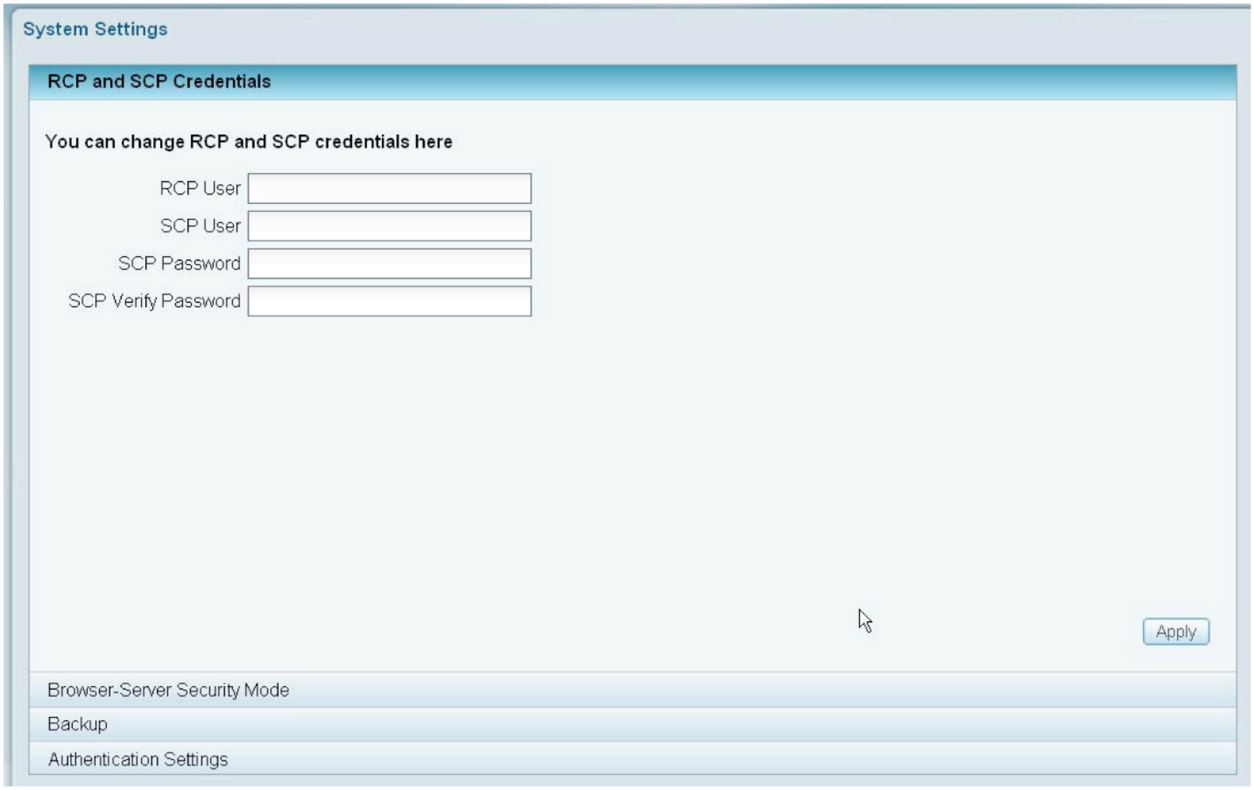
In this section you can set up the following:

1. RCP and SCP credentials for the LMS server when LMS uses these protocols
2. Browser-Server Security Mode
3. Backup-LMS backup directory location and schedule
4. Authentication Settings-You can choose from a number of authentication modes.

RCP and SCP Credentials

Use the System Settings window in Figure 18 to change the RCP and SCP credentials.

Figure 18. Changing the RCP and SCP Credentials



System Settings

RCP and SCP Credentials

You can change RCP and SCP credentials here

RCP User: Name used by a network device when it connects to CiscoWorks LMS server to run RCP. 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 network device when it connects to the CiscoWorks 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.

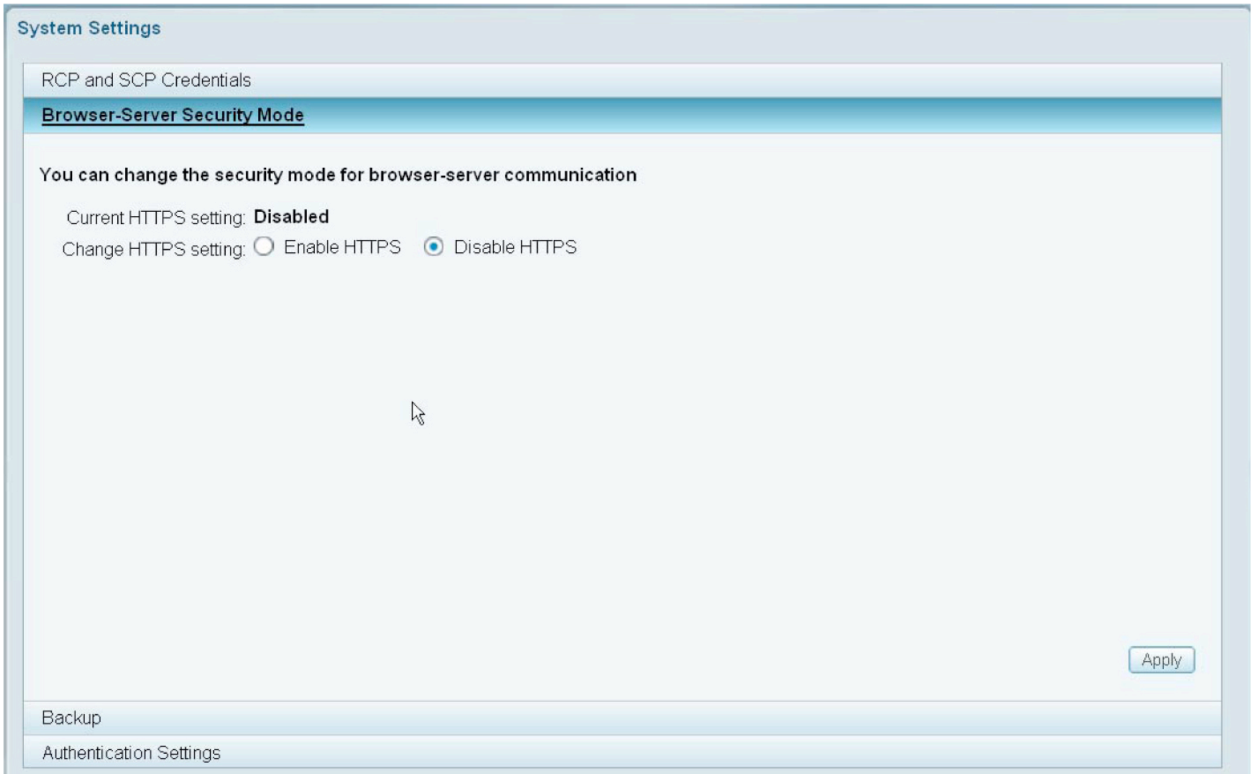
SCP Password: Enter the password for the SCP user in this field. The password you have entered here is used for authentication while transferring software images using SCP protocol. You must specify a username that has SSH authentication on a Solaris system. SCP uses this authentication for transferring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

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

Click **Apply**.

Browser-Server Security Mode

Figure 19. Changing the Security Mode for Browser Server Communication



You can change the security mode for browser-server communication

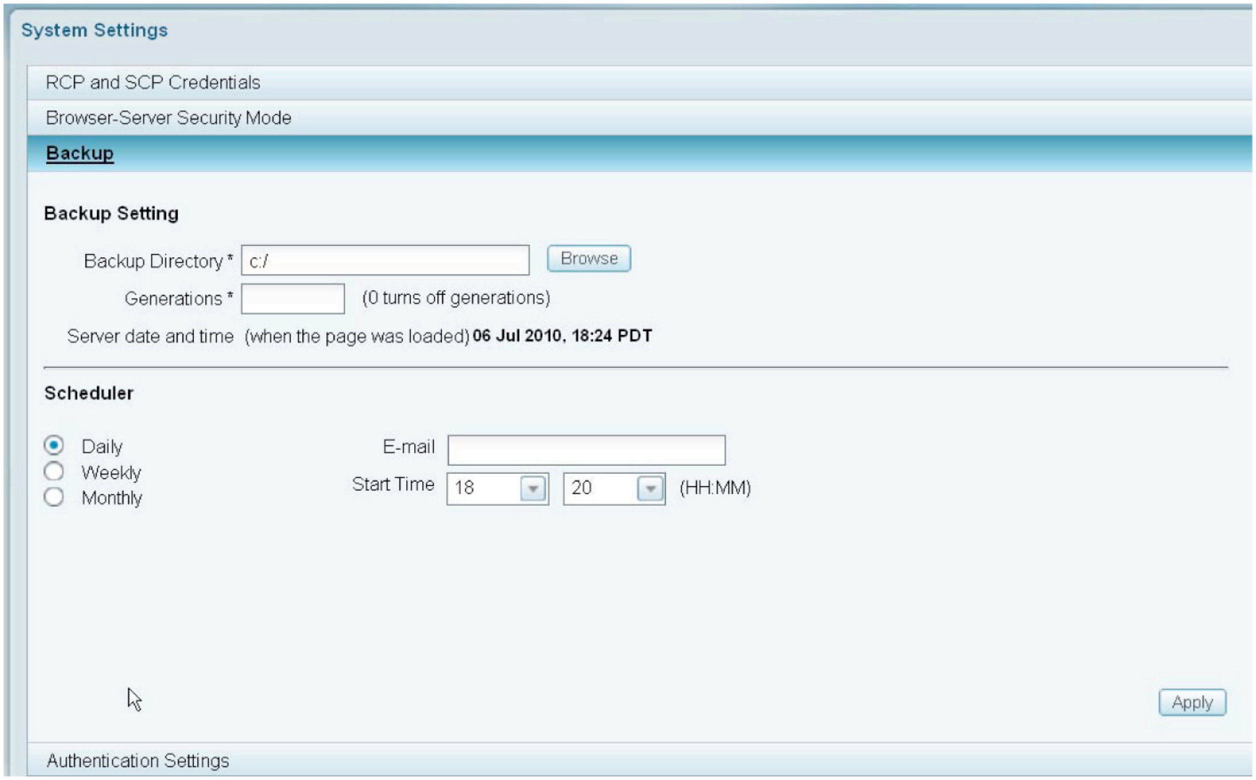
Current HTTPS setting: **Disabled**

Change HTTPS setting: ○ Enable HTTPS ● Disable HTTPS

In Figure 19, choose the HTTPS setting, either to enable or disable HTTPS.

Backup

Figure 20. Changing Backup Settings



System Settings

RCP and SCP Credentials

Browser-Server Security Mode

Backup

Backup Setting

Backup Directory * c:/ [Browse]

Generations * (0 turns off generations)

Server date and time (when the page was loaded) **06 Jul 2010, 18:24 PDT**

Scheduler

● Daily
○ Weekly
○ Monthly

E-mail

Start Time 18 20 (HH:MM)

[Apply]

Authentication Settings

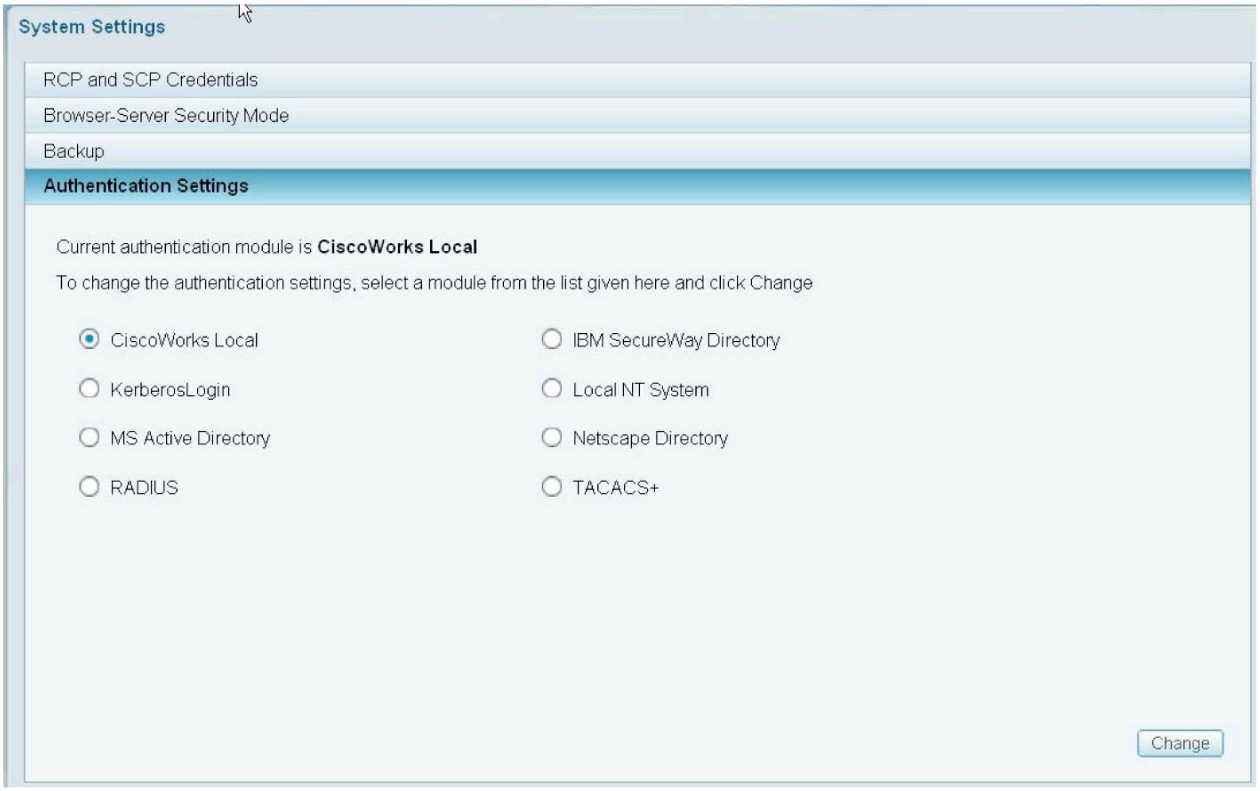
In the window shown in Figure 20, specify the location of the backup directory in the Backup Directory field and the maximum number of backups to be stored in the Generations field.

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

Authentication Settings

In the window shown in Figure 21, you can change the authentication settings.

Figure 21. Changing the Authentication Settings



Current authentication module is **CiscoWorks Local**

To change the authentication settings, select a module from the list given here and click Change

● CiscoWorks Local
○ IBM SecureWay Directory
○ KerberosLogin
○ Local NT System
○ MS Active Directory
○ Netscape Directory
○ RADIUS
○ TACACS+

Device Management

In this section there are two primary tasks: device management functions and how to add devices to 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 Addition** link.

Device Addition

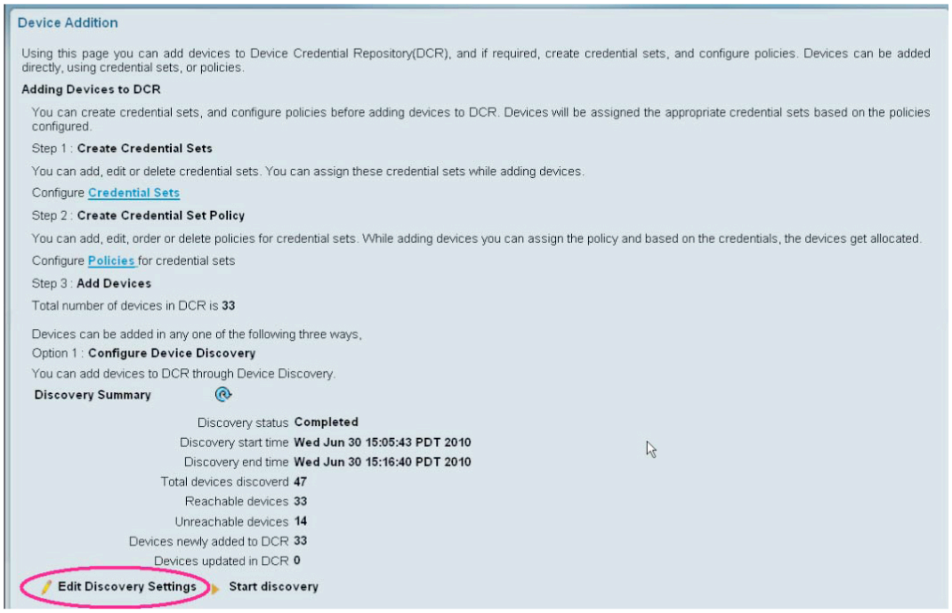
This is where you will add devices to be managed by LMS. There are three ways you can add devices in LMS:

1. Device discovery
2. Add devices manually
3. Import devices

We will discuss the device discovery option in detail.

> Click **Edit Discovery Settings**. Here you are going to set the discovery properties such as which discovery protocol to use, seed device settings and SNMP settings, and so on.

Figure 22. Setting Discovery Properties



Device Addition

Using this page you can add devices to Device Credential Repository(DCR), and if required, create credential sets, and configure policies. Devices can be added directly, using credential sets, or policies.

Adding Devices to DCR

You can create credential sets, and configure policies before adding devices to DCR. Devices will be assigned the appropriate credential sets based on the policies configured.

Step 1 : **Create Credential Sets**

You can add, edit or delete credential sets. You can assign these credential sets while adding devices.

Configure Credential Sets

Step 2 : **Create Credential Set Policy**

You can add, edit, order or delete policies for credential sets. While adding devices you can assign the policy and based on the credentials, the devices get allocated.

Configure Policies for credential sets

Step 3 : **Add Devices**

Total number of devices in DCR is **33**

Devices can be added in any one of the following three ways,

Option 1 : **Configure Device Discovery**

You can add devices to DCR through Device Discovery.

Discovery Summary

Discovery status **Completed**

Discovery start time **Wed Jun 30 15:05:43 PDT 2010**

Discovery end time **Wed Jun 30 15:16:40 PDT 2010**

Total devices discoverd **47**

Reachable devices **33**

Unreachable devices **14**

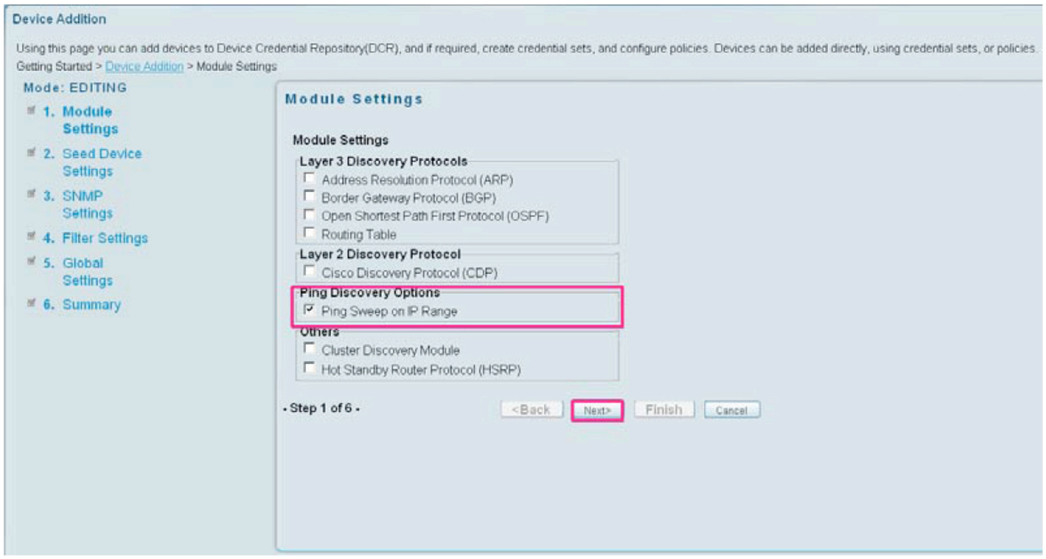
Devices newly added to DCR **33**

Devices updated in DCR **0**

Choose Ping Discovery Options by checking **Ping Sweep on IP Range**. See Figures 23-27.

Click **Next**.

Figure 23. Choosing Ping Discovery Options



Device Addition

Using this page you can add devices to Device Credential Repository(DCR), and if required, create credential sets, and configure policies. Devices can be added directly, using credential sets, or policies.

Getting Started > Device Addition > Module Settings

Module Settings

Module Settings

Layer 3 Discovery Protocols

☐ Address Resolution Protocol (ARP)

☐ Border Gateway Protocol (BGP)

☐ Open Shortest Path First Protocol (OSPF)

☐ Routing Table

Layer 2 Discovery Protocol

☐ Cisco Discovery Protocol (CDP)

Ping Discovery Options

☑ Ping Sweep on IP Range

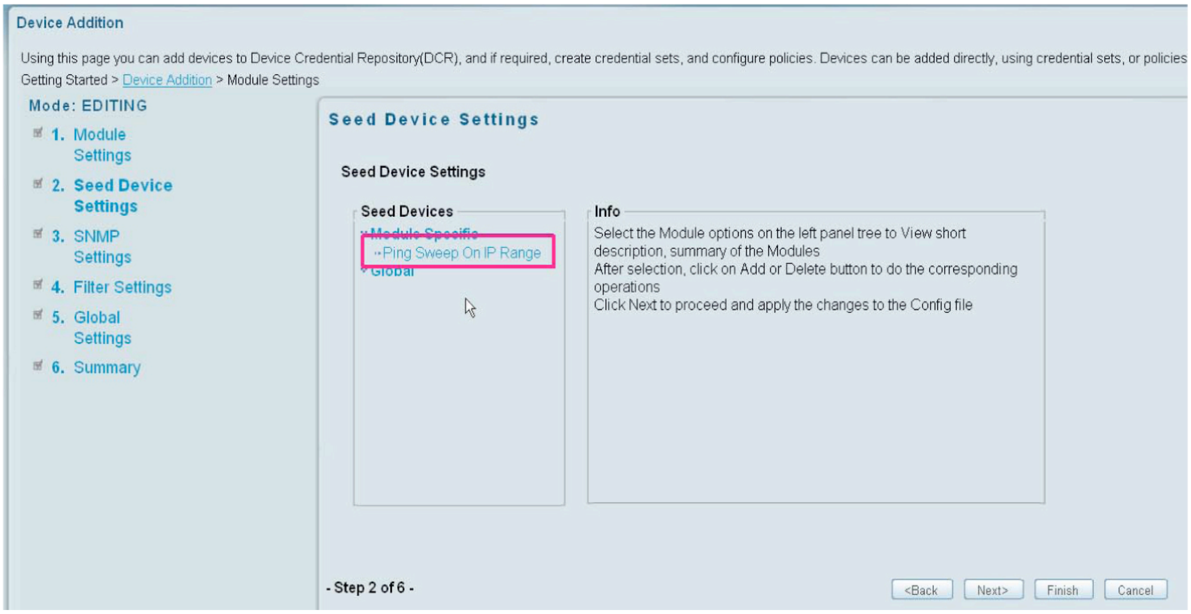
Others

☐ Cluster Discovery Module

☐ Hot Standby Router Protocol (HSRP)

- Step 1 of 6 -

Figure 24. The Device Addition Page



Device Addition

Using this page you can add devices to Device Credential Repository(DCR), and if required, create credential sets, and configure policies. Devices can be added directly, using credential sets, or policies

Getting Started > Device Addition > Module Settings

Mode: EDITING

1. Module Settings
2. Seed Device Settings
3. SNMP Settings
4. Filter Settings
5. Global Settings
6. Summary

Seed Device Settings

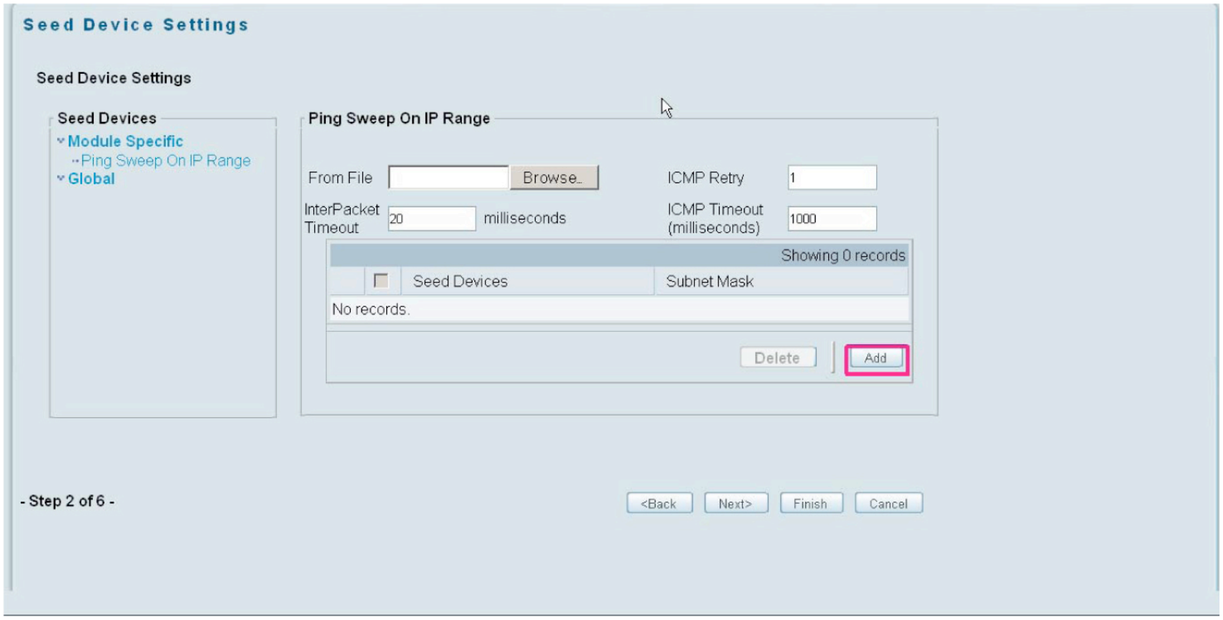
Seed Device Settings

Info

Select the Module options on the left panel tree to View short description, summary of the Modules
After selection, click on Add or Delete button to do the corresponding operations
Click Next to proceed and apply the changes to the Config file

- Step 2 of 6 -

Figure 25. Seed Device Settings Window-Clicking to Add a Device



Seed Device Settings

Seed Device Settings

Ping Sweep On IP Range

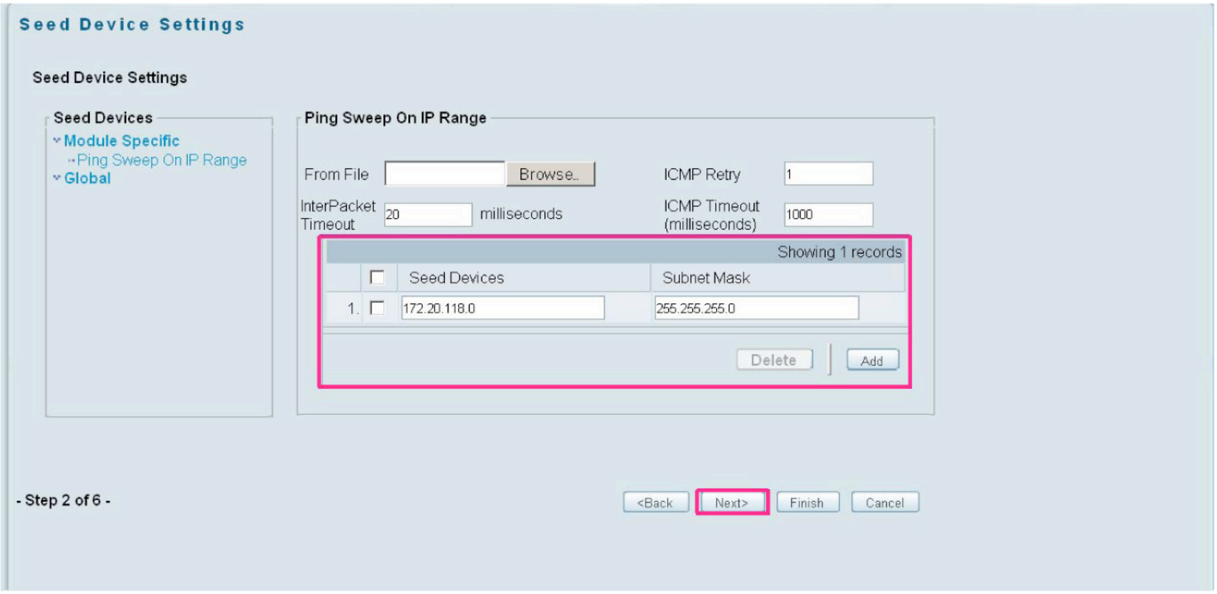
From File	Browse..	ICMP Retry	1
InterPacket Timeout	20 milliseconds	ICMP Timeout (milliseconds)	1000

Showing 0 records

□	Seed Devices	Subnet Mask
No records.		

- Step 2 of 6 -

Figure 26. Clicking Next to Proceed with Adding Devices



Seed Device Settings

Seed Device Settings

Seed Devices
- Module Specific
  - Ping Sweep On IP Range
- Global

Ping Sweep On IP Range

From File: [ ] Browse...

ICMP Retry: 1

InterPacket Timeout: 20 milliseconds

ICMP Timeout (milliseconds): 1000

Showing 1 records

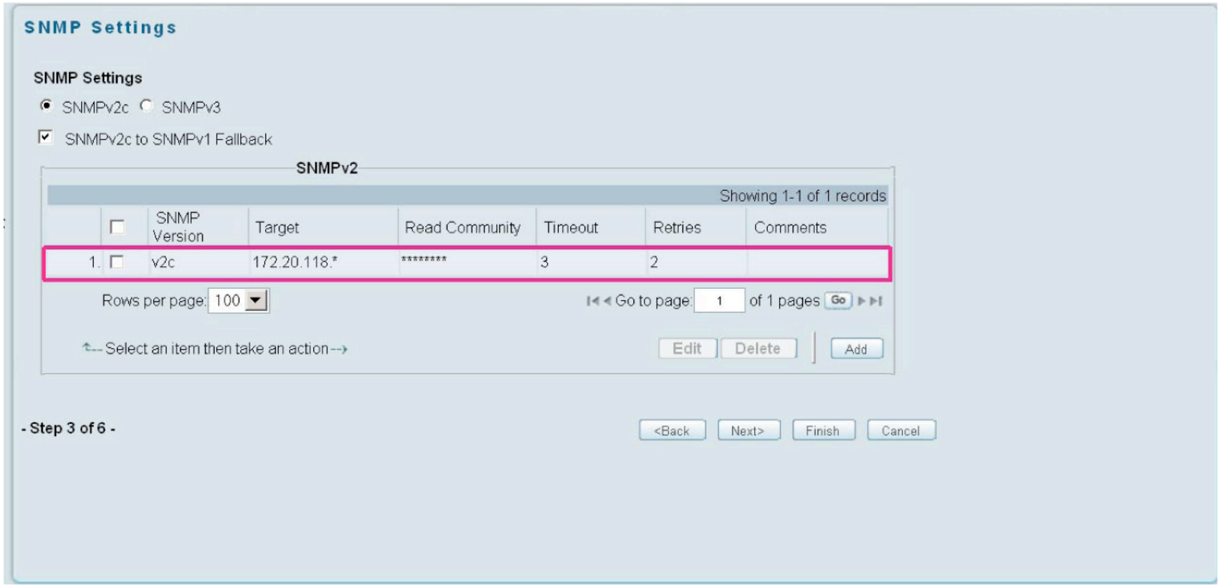
	□	Seed Devices	Subnet Mask
1.	□	172.20.118.0	255.255.255.0

Delete | Add

- Step 2 of 6 -

<Back | Next> | Finish | Cancel

Figure 27. Configuring the SNMP Settings



SNMP Settings

SNMP Settings

● SNMPv2c ○ SNMPv3

☑ SNMPv2c to SNMPv1 Fallback

SNMPv2

Showing 1-1 of 1 records

	□	SNMP Version	Target	Read Community	Timeout	Retries	Comments
1.	□	v2c	172.20.118.*	********	3	2	

Rows per page: 100 | Go to page: 1 of 1 pages Go

Select an item then take an action

Edit | Delete | Add

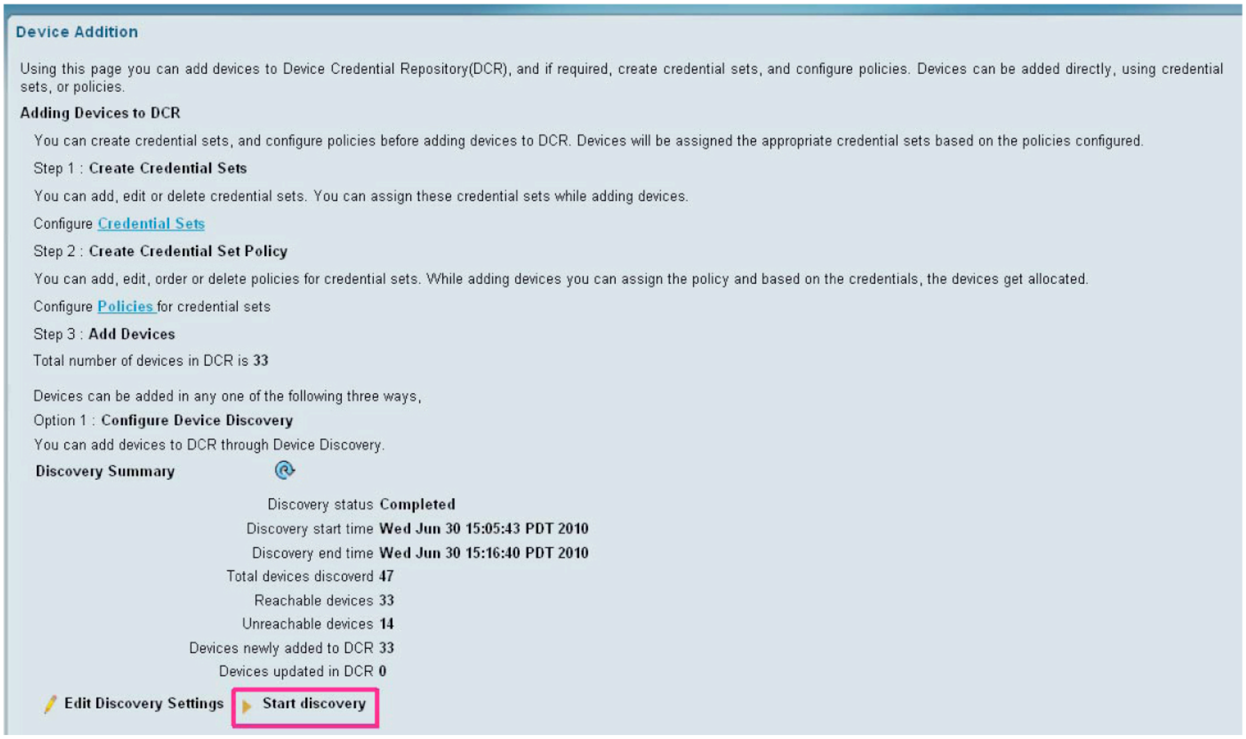
- Step 3 of 6 -

<Back | Next> | Finish | Cancel

Click **Finish**.

At this point, you are ready to start the discovery. See Figure 28.

Figure 28. Starting Discovery



Device Addition

Using this page you can add devices to Device Credential Repository(DCR), and if required, create credential sets, and configure policies. Devices can be added directly, using credential sets, or policies.

Adding Devices to DCR

You can create credential sets, and configure policies before adding devices to DCR. Devices will be assigned the appropriate credential sets based on the policies configured.

Step 1 : **Create Credential Sets**

You can add, edit or delete credential sets. You can assign these credential sets while adding devices.

Configure Credential Sets

Step 2 : **Create Credential Set Policy**

You can add, edit, order or delete policies for credential sets. While adding devices you can assign the policy and based on the credentials, the devices get allocated.

Configure Policies for credential sets

Step 3 : **Add Devices**

Total number of devices in DCR is **33**

Devices can be added in any one of the following three ways,

Option 1 : **Configure Device Discovery**

You can add devices to DCR through Device Discovery.

Discovery Summary

Discovery status	**Completed**
Discovery start time	**Wed Jun 30 15:05:43 PDT 2010**
Discovery end time	**Wed Jun 30 15:16:40 PDT 2010**
Total devices discoverd	**47**
Reachable devices	**33**
Unreachable devices	**14**
Devices newly added to DCR	**33**
Devices updated in DCR	**0**

LMS starts the discovery of the devices in the IP range and seed device specified, and the Discovery Summary is displayed.

Click Proceed to **Manage User Roles**.

User Management

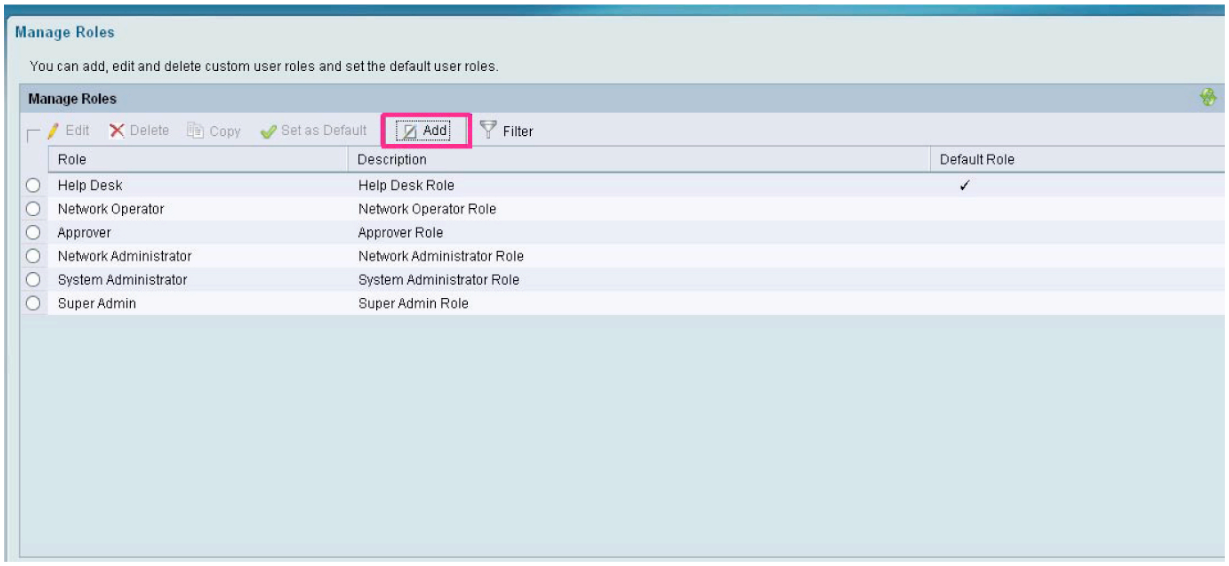
In this section, you can define user roles and, based on the user roles, you can define and add users.

User Roles

You can add your own custom user roles. LMS provides predefined roles and a default role. If you don’t need to define a custom role, please skip this subsection.

To define a custom user role, Myrole, follow the steps below as shown in Figure 29 and the following screenshots.

Figure 29. Adding a Role



Manage Roles

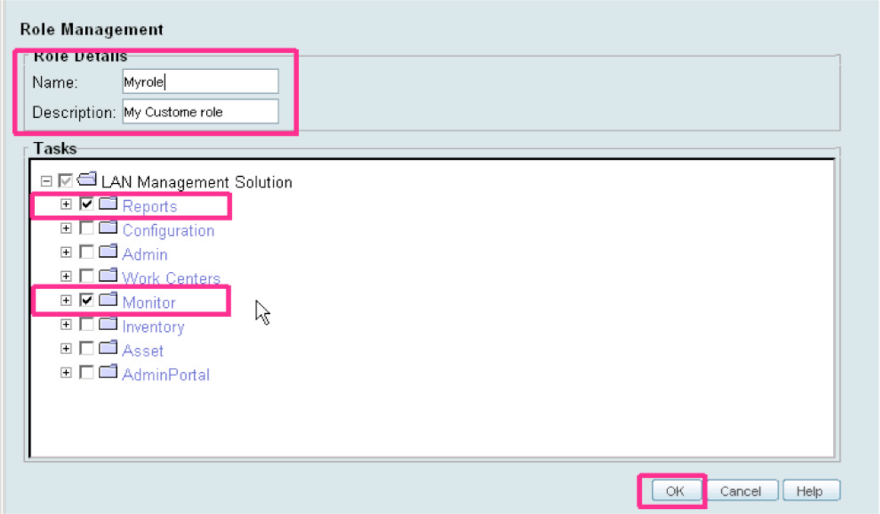
You can add, edit and delete custom user roles and set the default user roles.

Manage Roles

	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	
○	Super Admin	Super Admin Role	

Enter the role name as Myrole, enter some description, and choose the tasks that this role can execute. Here we are choosing **Reports** and **Monitor**. This will allow the role, Myrole, to perform only the reporting and monitoring functionality of LMS. See Figure 30.

Figure 30. Choosing Reports and Monitor for Myrole



Role Management

Role Details

Name: Myrole

Description: My Custome role

Tasks

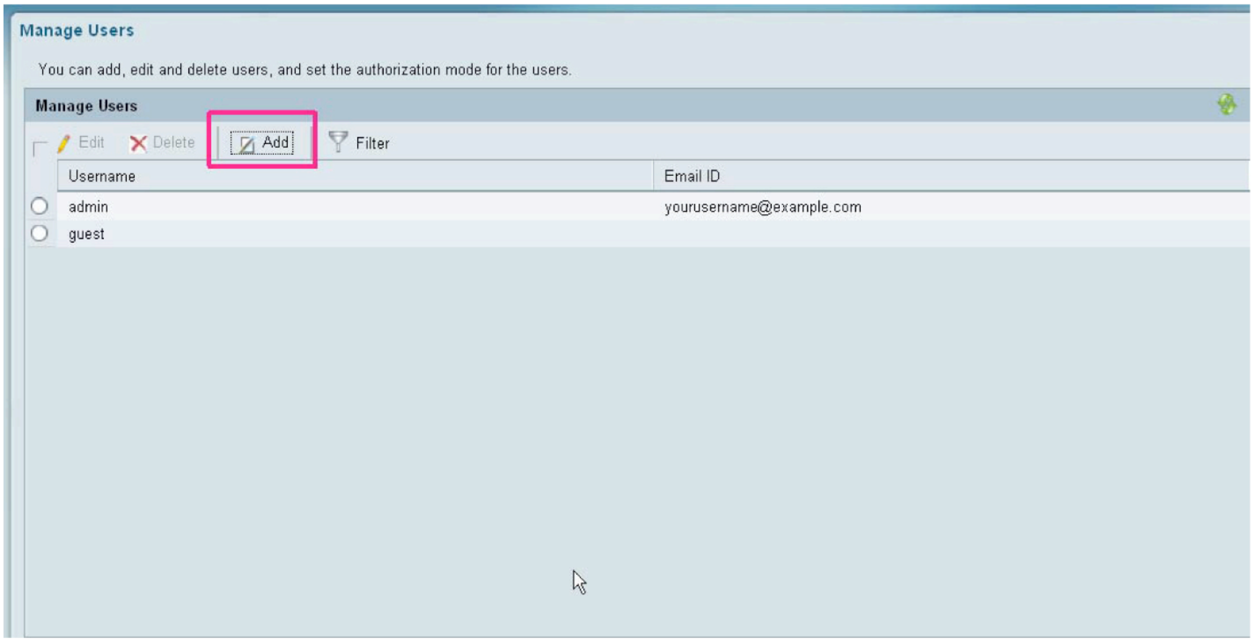
- ☑ LAN Management Solution
  - ☑ Reports
  - □ Configuration
  - □ Admin
  - □ Work Centers
  - ☑ Monitor
  - □ Inventory
  - □ Asset
  - □ AdminPortal

Adding Users

If you need to add users, please follow the workflow shown in Figures 31 and 32.

Here we are adding a user named joeuser, who has the roles **Network Operator** and **Approver**.

Figure 31. Adding a User



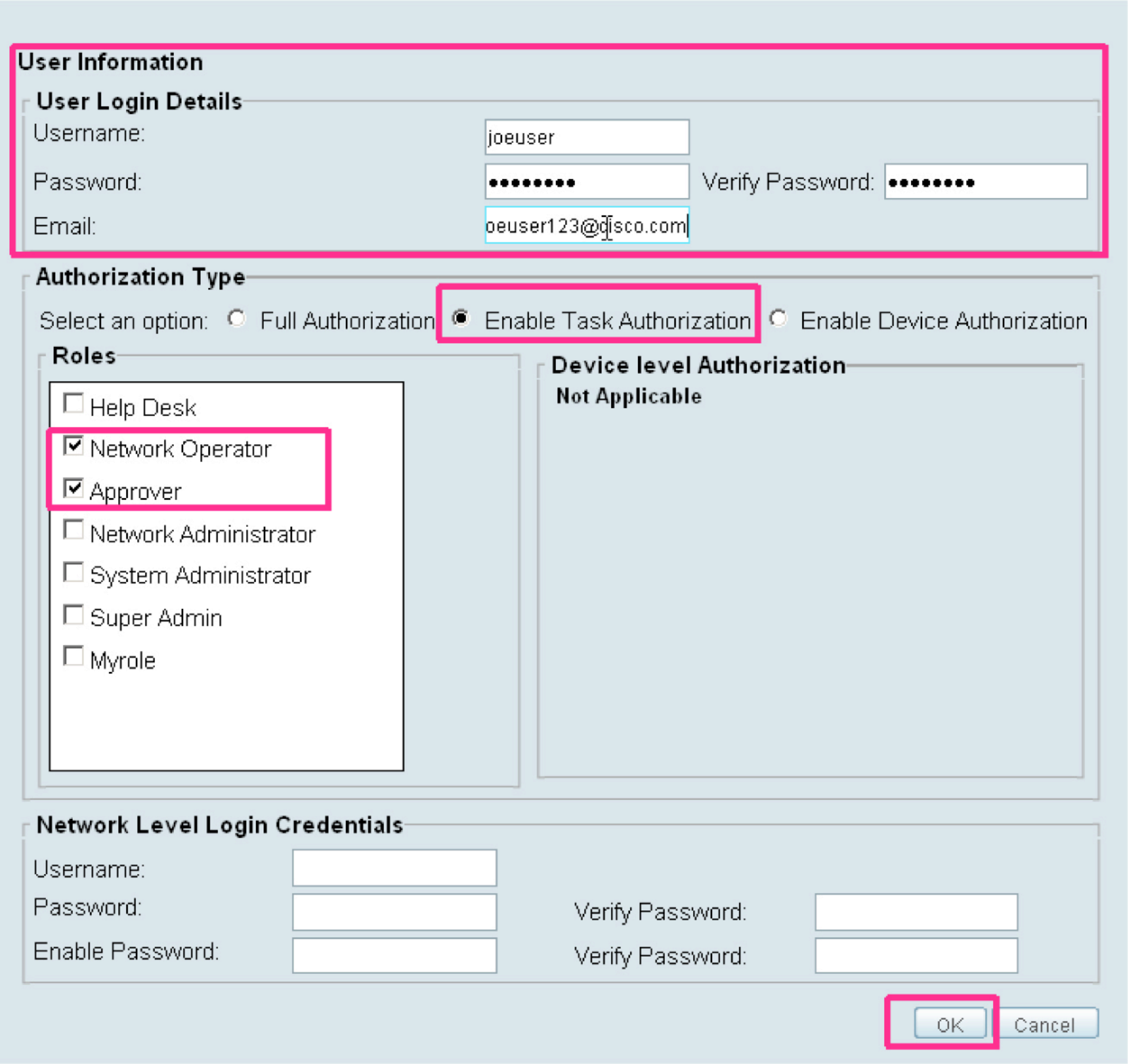
Manage Users

You can add, edit and delete users, and set the authorization mode for the users.

Manage Users

	Username	Email ID
○	admin	yourusername@example.com
○	guest	

Figure 32. Choosing Roles for the New User



User Information

User Login Details

Username: joeuser

Password: •••••••• Verify Password: ••••••••

Email: oeuser123@cisco.com

Authorization Type

Select an option: ○ Full Authorization ● Enable Task Authorization ○ Enable Device Authorization

Roles

- □ Help Desk
- ☑ Network Operator
- ☑ Approver
- □ Network Administrator
- □ System Administrator
- □ Super Admin
- □ Myrole

Device level Authorization

Not Applicable

Network Level Login Credentials

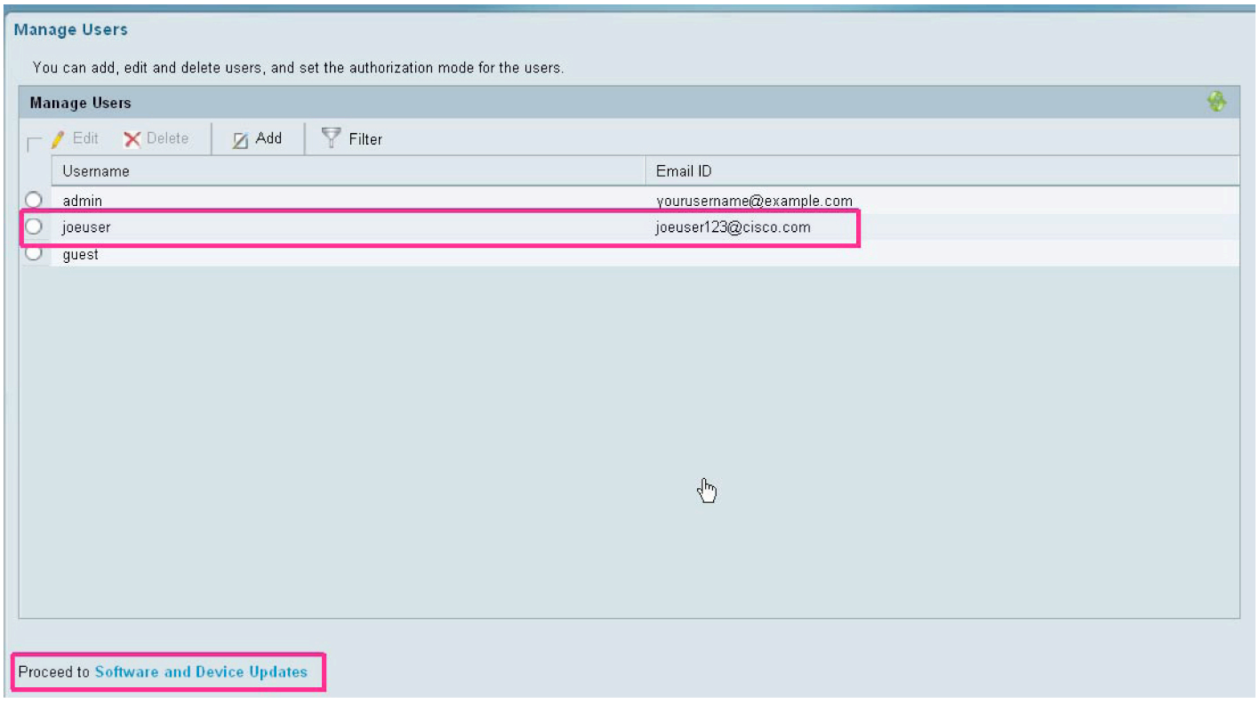
Username:

Password: Verify Password:

Enable Password: Verify Password:

As you can see, the user joeuser has been added (Figure 33).

Figure 33. Verifying the New User



Manage Users

You can add, edit and delete users, and set the authorization mode for the users.

Manage Users

	Username	Email ID
○	admin	yourusername@example.com
○	joeuser	joeuser123@cisco.com
○	guest	

Proceed to Software and Device Updates

Software and Device Updates

LMS periodically releases software and device package updates. You can check for these updates from Cisco.com and download them to a location on your server. You can install these updates from this location.

In the case of device updates, you can install the updates using a web-based user interface and the command-line interface, wherever possible. Most of the device family-based packages can be installed directly from the web interface while the device support packages such as Incremental Device Update (IDU) have to be installed based on the installation instructions in the respective Readme files.

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

Advanced Configurations

Monitoring Configurations

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 4.0* 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 4.0* for 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 4.0* for more information.

Inventory and Configuration Management

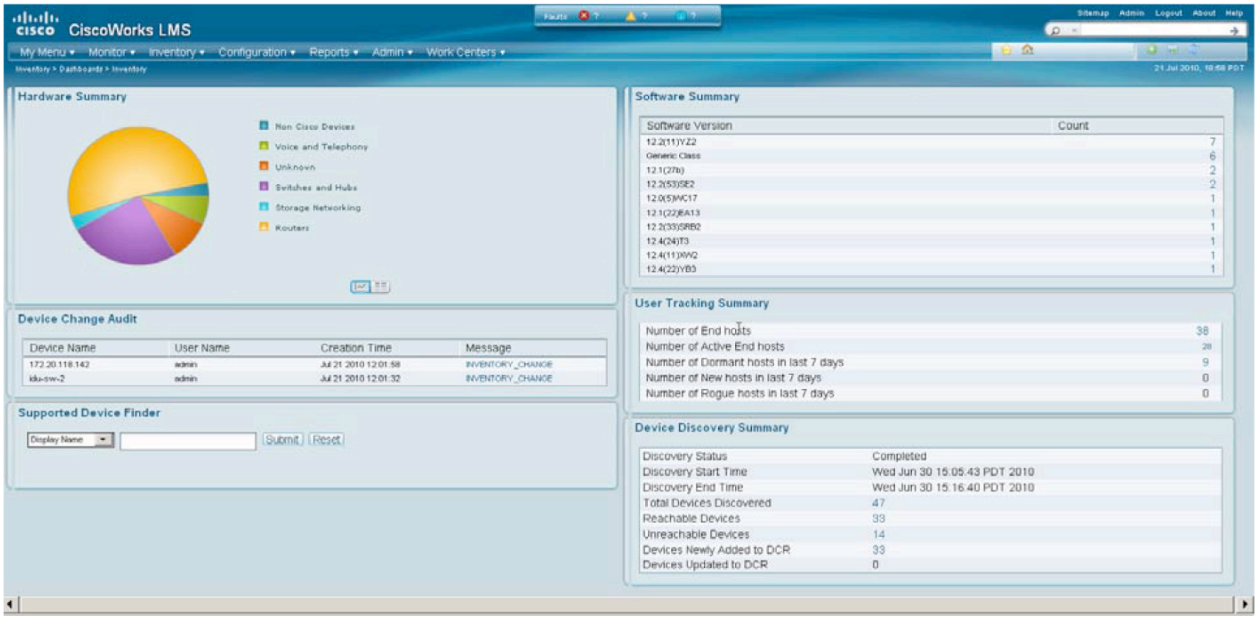
Business Scenarios

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 4.0, 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 one-by-one 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?

Figure 34 provides an inventory of devices.

Figure 34. Inventory Dashboard



Hardware Summary

Device Change Audit

Device Name	User Name	Creation Time	Message
172.20.118.142	admin	Jul 21 2010 12:01:58	INVENTORY_CHANGE
idu-sw-2	admin	Jul 21 2010 12:01:32	INVENTORY_CHANGE

Supported Device Finder

Software Summary

Software Version	Count
12.2(11)YZ2	7
Generic Class	6
12.1(27b)	2
12.2(53)SE2	2
12.0(5)WC17	1
12.1(22)EA13	1
12.2(33)SRB2	1
12.4(24)T3	1
12.4(11)XW2	1
12.4(22)YB3	1

User Tracking Summary

Number of End hosts	38
Number of Active End hosts	28
Number of Dormant hosts in last 7 days	9
Number of New hosts in last 7 days	0
Number of Rogue hosts in last 7 days	0

Device Discovery Summary

Discovery Status	Completed
Discovery Start Time	Wed Jun 30 15:05:43 PDT 2010
Discovery End Time	Wed Jun 30 15:16:40 PDT 2010
Total Devices Discovered	47
Reachable Devices	33
Unreachable Devices	14
Devices Newly Added to DCR	33
Devices Updated to DCR	0

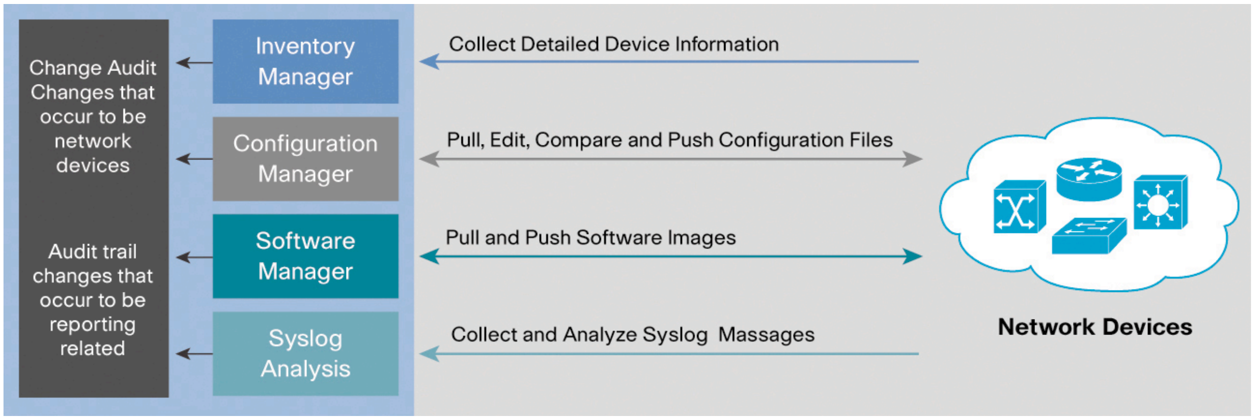
Configuration and Inventory Management

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 (Figure 35). Resource Manager Essentials (RME) consists of the following major components:

- **Inventory Manager:** Builds and maintains an up-to-date hardware and software inventory providing reports on detailed inventory information. LMS has many predefined reports. You can also create custom reports to dig out just the information you need.
- **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.

Figure 35. Configuration and Inventory Management Functions


Change Audit Changes that occur to be network devices
Audit trail changes that occur to be reporting related
Inventory Manager
Configuration Manager
Software Manager
Syslog Analysis
Collect Detailed Device Information
Pull, Edit, Compare and Push Configuration Files
Pull and Push Software Images
Collect and Analyze Syslog Massages
Network Devices

Inventory Management

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.

Third-party support has been added for Inventory management in LMS 4.0. LMS 4.0 can poll some basic information on third-party devices, which helps users to get a complete picture of the overall network inventory.

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 time stamp has changed. If there is a change in the time stamp, 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.

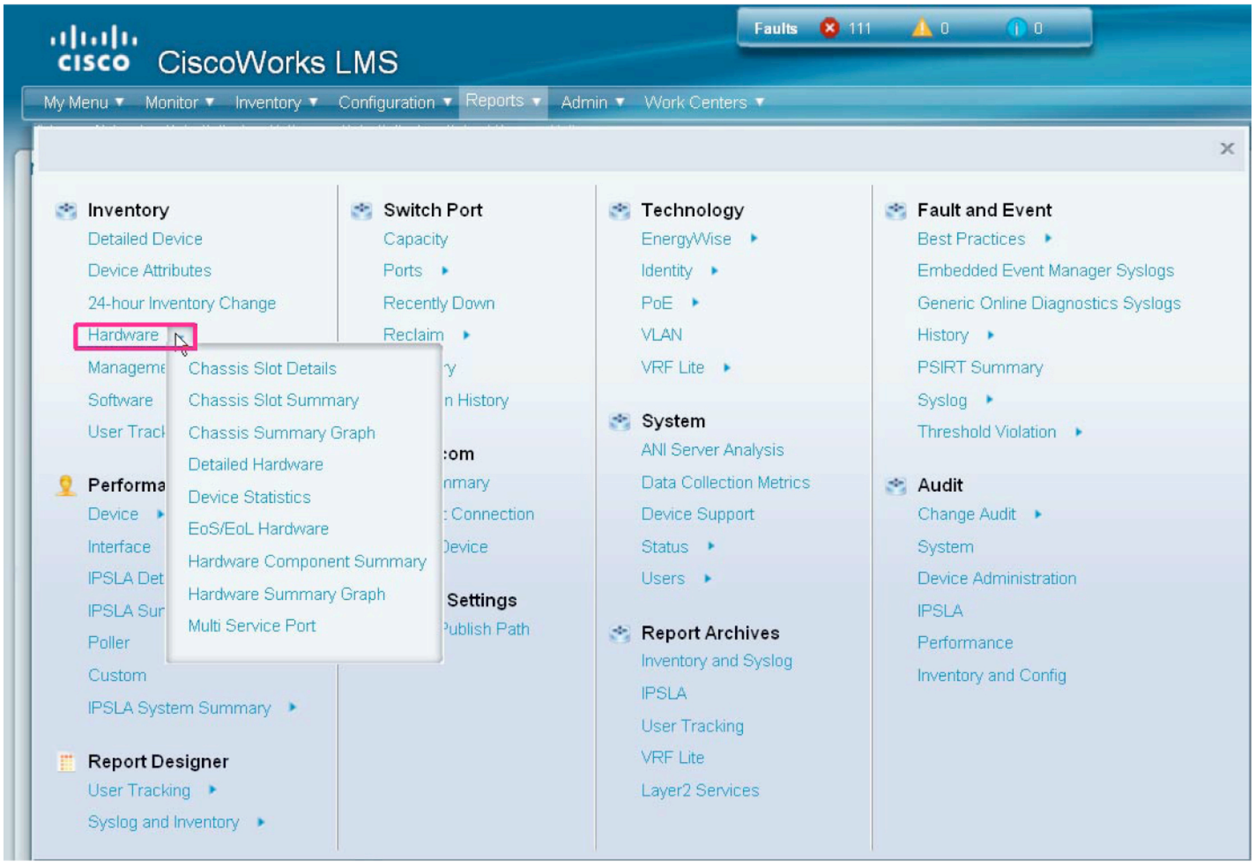
The predefined default periodicity of the collector job is once a week, and the predefined default periodicity of the polling job is once a day.

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

Inventory Reports

LMS starts retrieving inventory information based on the default schedule setting. LMS has numerous predefined reports for Inventory (Figure 36). These reports can be viewed by going to **Reports → Inventory → Hardware**.

Figure 36. Inventory Reports



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

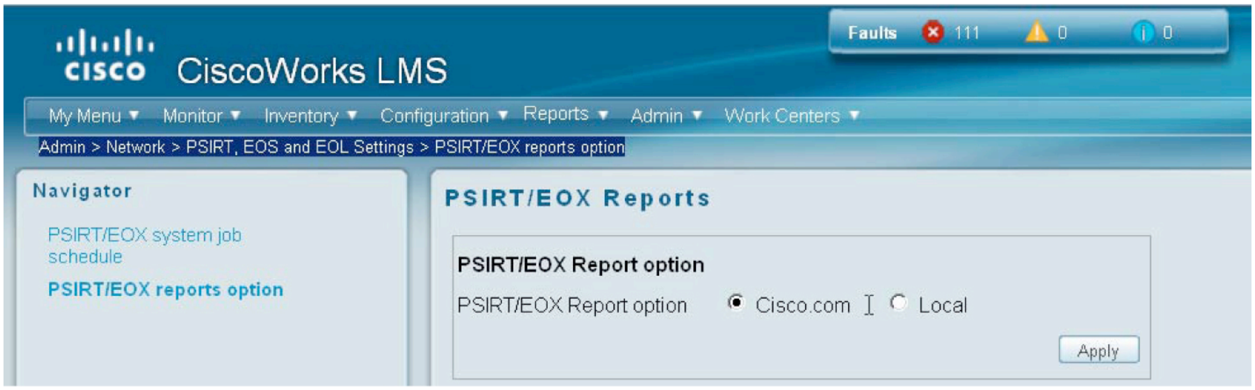
All these reports are generated with a set of predefined query criteria. For example, Software Report will list the software versions based on the categories of the devices. If you want to query a customized list of variables from the inventory, you can use a custom reports template for this as described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

  In LMS 3.1, offline support for PSIRT/EOX was added. Users can select the source of the information to be from Cisco Connection Online or a local file if the LMS server is not directly connected to the Internet. This can be customized at **Admin → Network → PSIRT, EOS and EOL Settings → PSIRT/EOX** reports option (Figure 37).

Figure 37. End of Sale/End of Life Hardware Report



CiscoWorks LMS
Faults 111 0 0
My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾
Admin > Network > PSIRT, EOS and EOL Settings > PSIRT/EOX reports option
Navigator
PSIRT/EOX system job schedule
PSIRT/EOX reports option

PSIRT/EOX Reports

PSIRT/EOX Report option

PSIRT/EOX Report option ● Cisco.com ○ Local

Apply

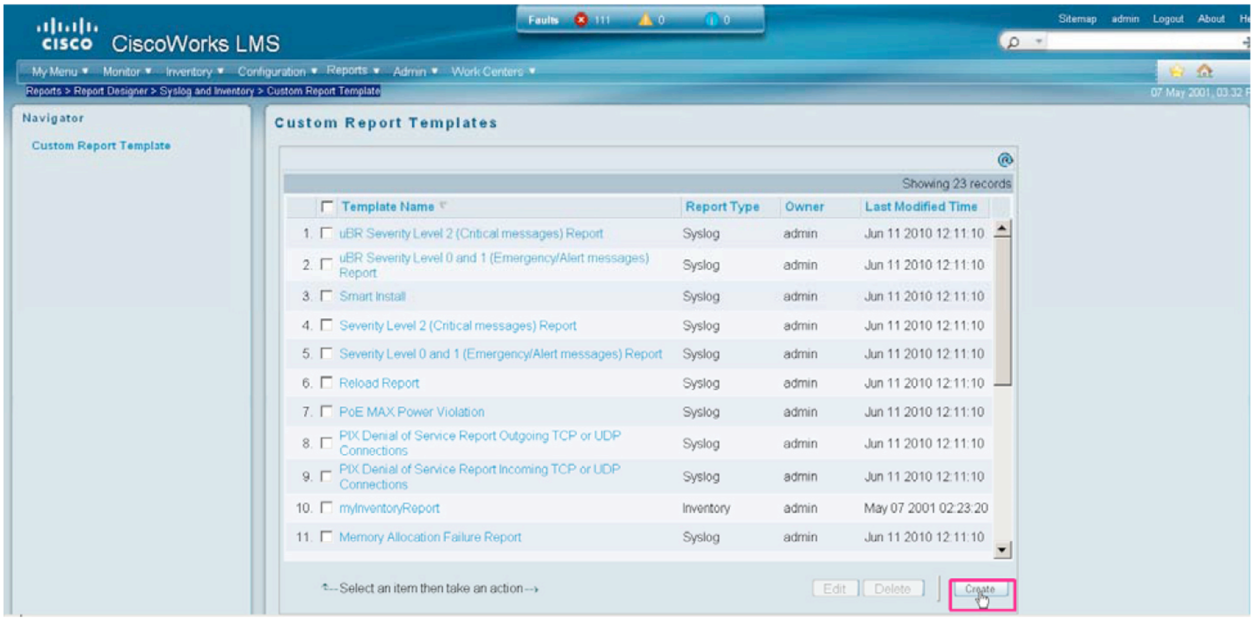
Check the online help to learn how to download Cisco Connection Online PSIRT/EoX information to a local file.

Custom Reports

To create a customized report (Figre 38) with your interested query variables, such as “the serial number of all c1701 routers”, follow these steps:

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

Figure 38. Custom Report Template



CiscoWorks LMS
Faults 111 0 0
Sitemap admin Logout About
My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾
Reports > Report Designer > Syslog and Inventory > Custom Report Template
07 May 2001, 03:32
Navigator
Custom Report Template

Custom Report Templates

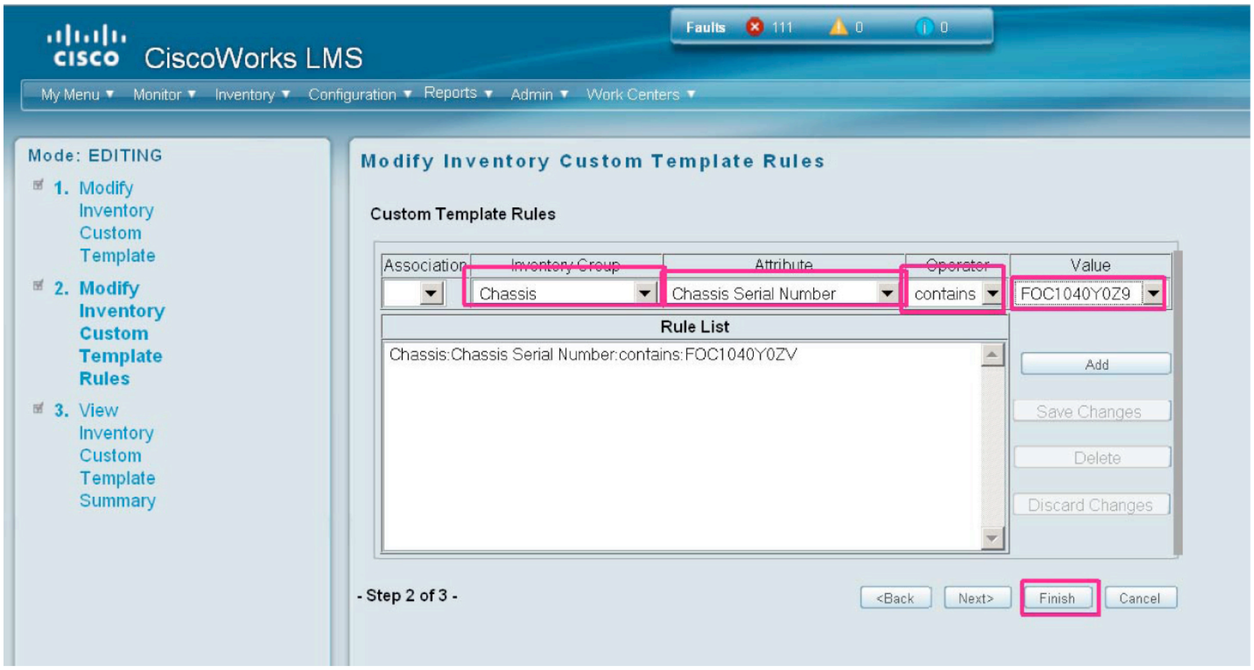
Showing 23 records

	□ Template Name	Report Type	Owner	Last Modified Time
1.	□ uBR Severity Level 2 (Critical messages) Report	Syslog	admin	Jun 11 2010 12:11:10
2.	□ uBR Severity Level 0 and 1 (Emergency/Alert messages) Report	Syslog	admin	Jun 11 2010 12:11:10
3.	□ Smart Install	Syslog	admin	Jun 11 2010 12:11:10
4.	□ Severity Level 2 (Critical messages) Report	Syslog	admin	Jun 11 2010 12:11:10
5.	□ Severity Level 0 and 1 (Emergency/Alert messages) Report	Syslog	admin	Jun 11 2010 12:11:10
6.	□ Reload Report	Syslog	admin	Jun 11 2010 12:11:10
7.	□ PoE MAX Power Violation	Syslog	admin	Jun 11 2010 12:11:10
8.	□ PIX Denial of Service Report Outgoing TCP or UDP Connections	Syslog	admin	Jun 11 2010 12:11:10
9.	□ PIX Denial of Service Report Incoming TCP or UDP Connections	Syslog	admin	Jun 11 2010 12:11:10
10.	□ myInventoryReport	Inventory	admin	May 07 2001 02:23:20
11.	□ Memory Allocation Failure Report	Syslog	admin	Jun 11 2010 12:11:10

In the next screen, give a name such as **myInventoryReport** and choose **Private**. Click **Next**.

2. Fill in the values as shown in Figure 39 to generate a custom report for chassis serial number .

Figure 39. Custom Chassis Serial Number Report



Mode: EDITING

1. Modify Inventory Custom Template
2. Modify Inventory Custom Template Rules
3. View Inventory Custom Template Summary

Modify Inventory Custom Template Rules

Custom Template Rules

Association	Inventory Group	Attribute	Operator	Value
	Chassis	Chassis Serial Number	contains	FOC1040Y0Z9

Rule List

Chassis:Chassis Serial Number:contains:FOC1040Y0ZV

- Step 2 of 3 -

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

3. Select **Reports → Inventory → myInventoryReport**.
4. 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

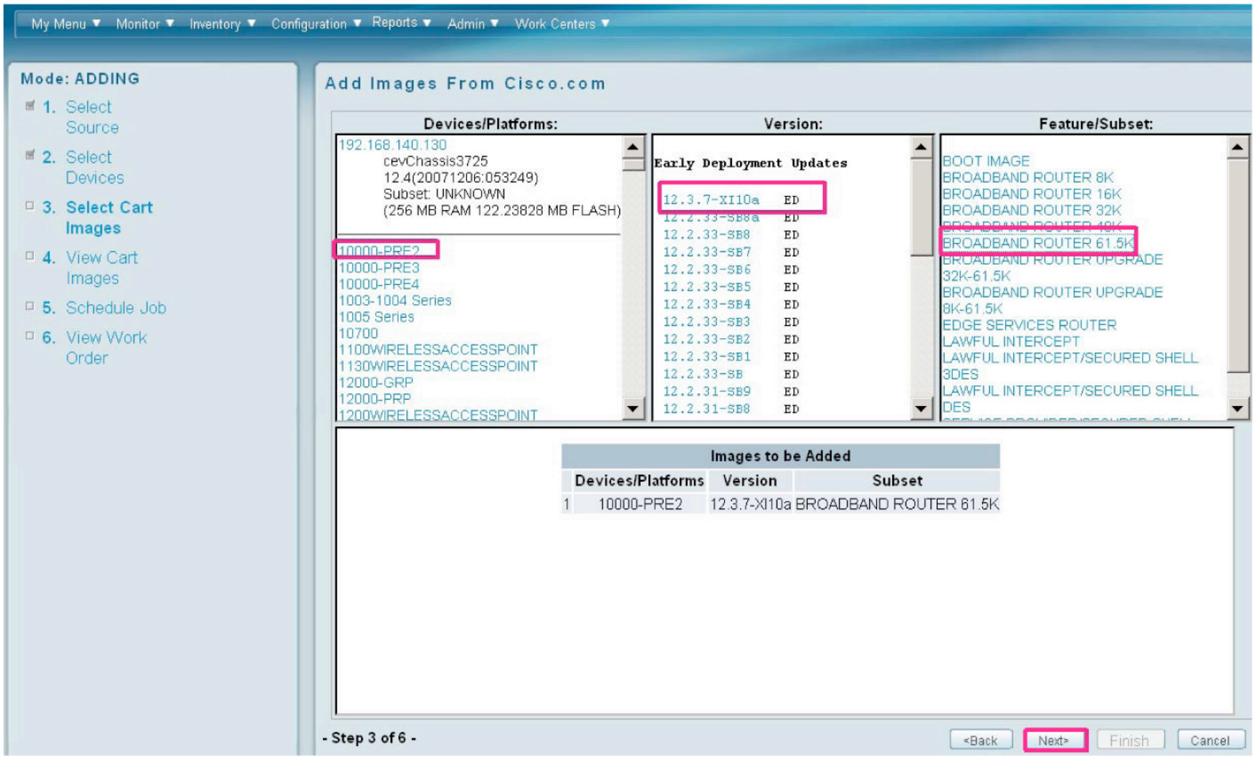
LMS greatly simplifies the work for software image management by building intelligence into the application to help the user pick and access device images from Cisco.com. Follow these steps to perform a software upgrade to your devices.

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 40). You can schedule the download immediately or later.

Configuration → Tools → Software Image Management → Software Repository

Note: You can also export the image from the local repository to be used elsewhere.

Figure 40. The Software Repository



Add Images From Cisco.com

Devices/Platforms:

192.168.140.130
cevChassis3725
12.4(20071206:053249)
Subset: UNKNOWN
(256 MB RAM 122.23828 MB FLASH)

10000-PRE2
10000-PRE3
10000-PRE4
1003-1004 Series
1005 Series
10700
1100WIRELESSACCESSPOINT
1130WIRELESSACCESSPOINT
12000-GRP
12000-PRP
1200WIRELESSACCESSPOINT

Version:

```
Early Deployment Updates
12.3.7-XI10a    ED
12.2.33-SB8a    ED
12.2.33-SB8     ED
12.2.33-SB7     ED
12.2.33-SB6     ED
12.2.33-SB5     ED
12.2.33-SB4     ED
12.2.33-SB3     ED
12.2.33-SB2     ED
12.2.33-SB1     ED
12.2.33-SB      ED
12.2.31-SB9     ED
12.2.31-SB8     ED
```

Feature/Subset:

BOOT IMAGE
BROADBAND ROUTER 8K
BROADBAND ROUTER 16K
BROADBAND ROUTER 32K
BROADBAND ROUTER 48K
BROADBAND ROUTER 61.5K
BROADBAND ROUTER UPGRADE
32K-61.5K
BROADBAND ROUTER UPGRADE
8K-61.5K
EDGE SERVICES ROUTER
LAWFUL INTERCEPT
LAWFUL INTERCEPT/SECURED SHELL
3DES
LAWFUL INTERCEPT/SECURED SHELL
DES

Images to be Added

	Devices/Platforms	Version	Subset
1	10000-PRE2	12.3.7-XI10a	BROADBAND ROUTER 61.5K

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 Archives Management

The Configuration Management tab in RME includes three 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

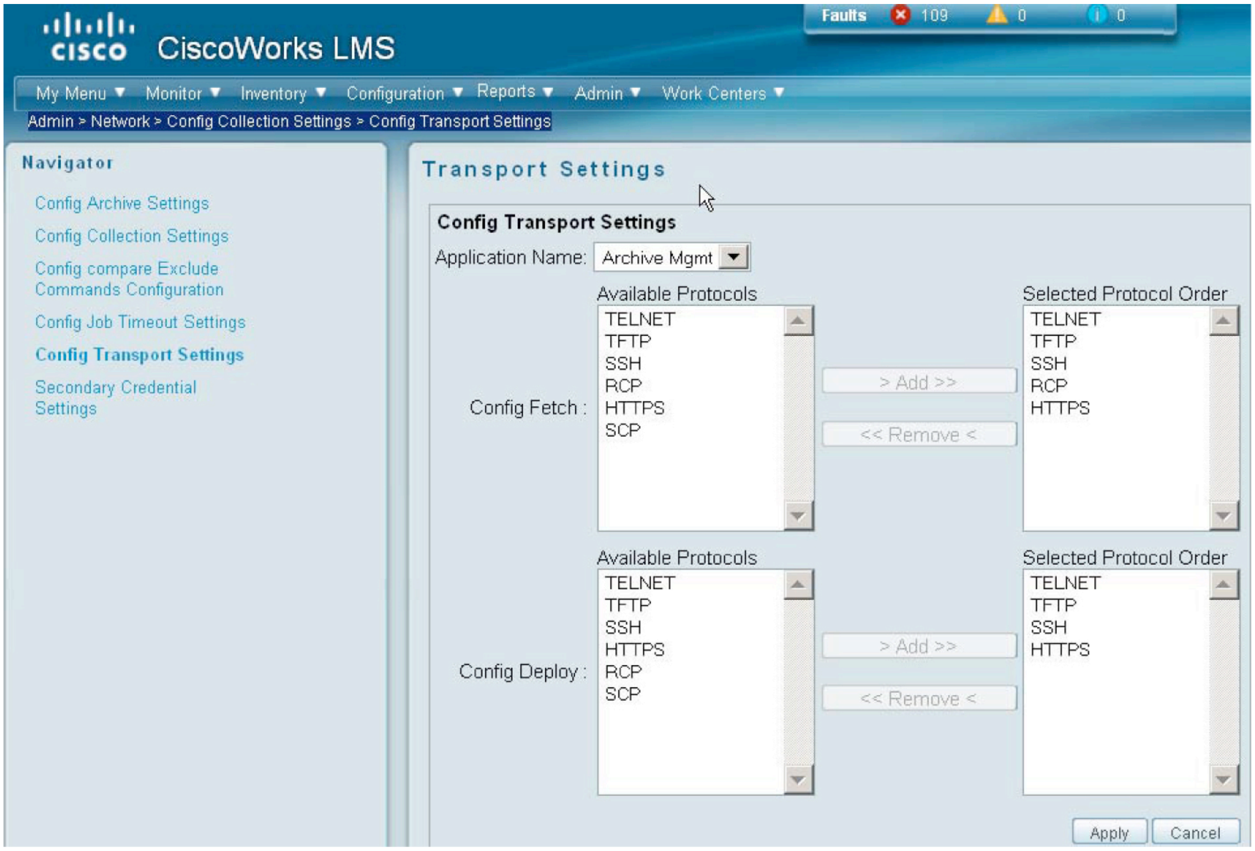
- Default protocols are used for a configuration fetch and deploy.
- Many protocols are used for performing a configuration fetch and deploy. The system provides a default order of protocols that will be used to fetch or deploy the configuration on the device. You can set the protocols and order for 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

To set up protocol ordering for Configuration Management (Figure 41), go to Admin → **Network** → Config Collection Settings → Config Transport Settings.

Figure 41. Setting Up Protocol Ordering for Configuration Management


CiscoWorks LMS
Faults 109 0 0
My Menu ▼ Monitor ▼ Inventory ▼ Configuration ▼ Reports ▼ Admin ▼ Work Centers ▼
Admin > Network > Config Collection Settings > Config Transport Settings
Navigator
Config Archive Settings
Config Collection Settings
Config compare Exclude Commands Configuration
Config Job Timeout Settings
Config Transport Settings
Secondary Credential Settings
Transport Settings
> Add >>
<< Remove <
Apply
Cancel

Config Transport Settings

Application Name: Archive Mgmt

Config Fetch :

Available Protocols	Selected Protocol Order
TELNET	TELNET
TFTP	TFTP
SSH	SSH
RCP	RCP
HTTPS	HTTPS
SCP	

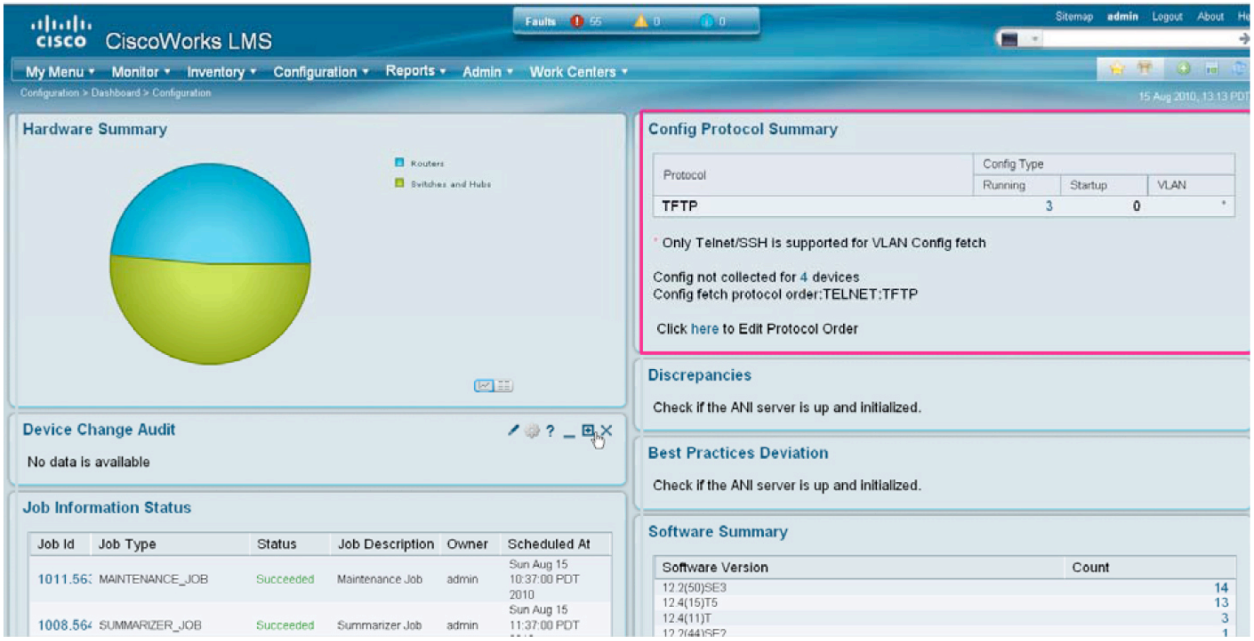
Config Deploy :

Available Protocols	Selected Protocol Order
TELNET	TELNET
TFTP	TFTP
SSH	SSH
HTTPS	HTTPS
RCP	
SCP	

Protocol ordering can be set up for different configuration applications (Archive Management, Config Editor, and NetConfig) by selecting the application from the **Application Name** drop-down list. Select the protocol order by using the **Add** and **Remove** buttons on the screen and click **Apply**.

You can view protocol ordering for Configuration Management in the Configuration Dashboard (Figure 42).

Figure 42. Viewing Protocol Ordering for Configuration Management in the Configuration Dashboard



Config Protocol Summary

Protocol	Config Type		
	Running	Startup	VLAN
TFTP	3	0	*

* Only Telnet/SSH is supported for VLAN Config fetch

Config not collected for 4 devices
Config fetch protocol order:TELNET:TFTP

Click here to Edit Protocol Order

Discrepancies

Check if the ANI server is up and initialized.

Device Change Audit

No data is available

Best Practices Deviation

Check if the ANI server is up and initialized.

Job Information Status

Job Id	Job Type	Status	Job Description	Owner	Scheduled At
1011.56:	MAINTENANCE_JOB	Succeeded	Maintenance Job	admin	Sun Aug 15 10:37:00 PDT 2010
1008.56‹	SUMMARIZER_JOB	Succeeded	Summarizer Job	admin	Sun Aug 15 11:37:00 PDT

Software Summary

Software Version	Count
12.2(50)SE3	14
12.4(15)T5	13
12.4(11)T	3
12.2(44)SE2	1

Config Editor

You can use the Config Editor application to perform the tasks listed in Table 6.

Table 6. 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 7.

Table 7. NetConfig Tasks

Task	Launch Point
• View and create NetConfig jobs using the NetConfig Job Browser. • 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	Configuration → **Job Browsers** → NetConfig
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

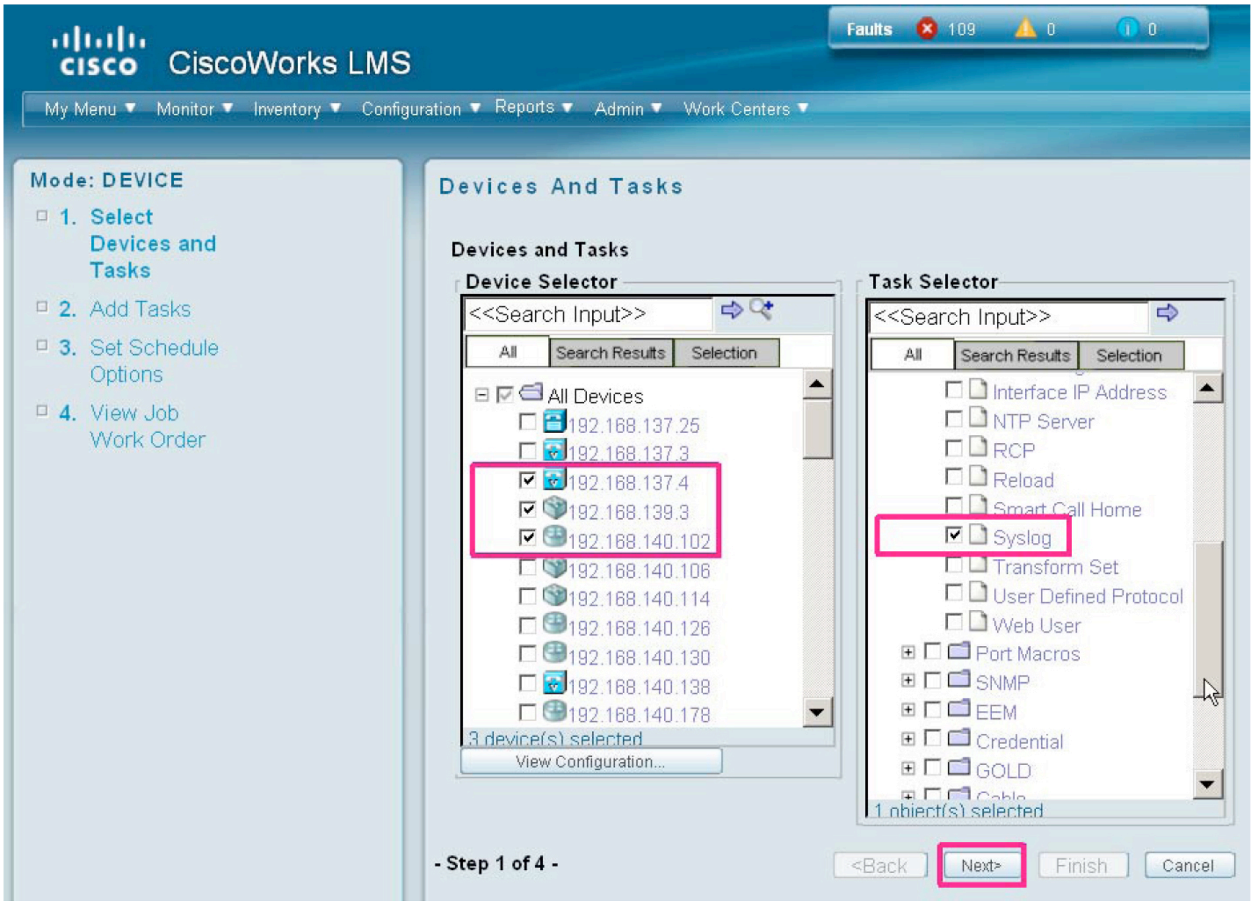
The NetConfig function provides a set of command templates that can be used to update the device configuration on multiple devices all at once. The NetConfig tool provides wizard-based templates to simplify and reduce the time it takes to roll out global changes to network devices. These templates can 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 → t, and click Create.
2. Choose **Device Based**.
3. Click **Go**.

See Figure 43.

Figure 43. Configuring the LMS Server



Device Selector:

- ⊟ ☑ All Devices
- ☐ 192.168.137.25
- ☐ 192.168.137.3
- ☑ 192.168.137.4
- ☑ 192.168.139.3
- ☑ 192.168.140.102
- ☐ 192.168.140.106
- ☐ 192.168.140.114
- ☐ 192.168.140.126
- ☐ 192.168.140.130
- ☐ 192.168.140.138
- ☐ 192.168.140.178

3 device(s) selected

Task Selector:

- ☐ Interface IP Address
- ☐ NTP Server
- ☐ RCP
- ☐ Reload
- ☐ Smart Call Home
- ☑ Syslog
- ☐ Transform Set
- ☐ User Defined Protocol
- ☐ Web User
- ⊞ ☐ Port Macros
- ⊞ ☐ SNMP
- ⊞ ☐ EEM
- ⊞ ☐ Credential
- ⊞ ☐ GOLD
- ⊞ ☐ Cable

1 object(s) selected

4. Choose the devices on which you want to enable the syslog functionality from the Device Selector.
5. Choose **General**, choose subselector **syslog**, and click **Next**.

See Figures 44 and 45.

Figure 44. Adding the Syslog Functionality

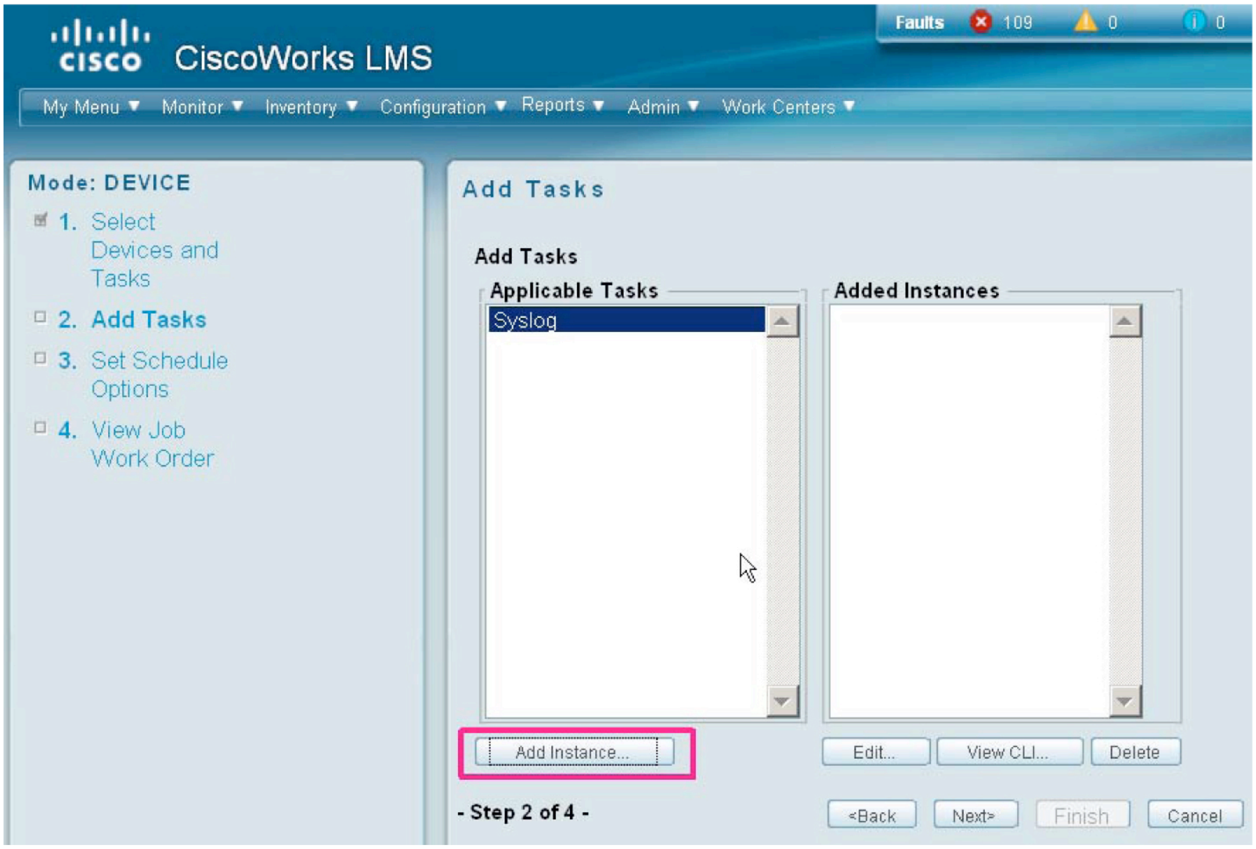
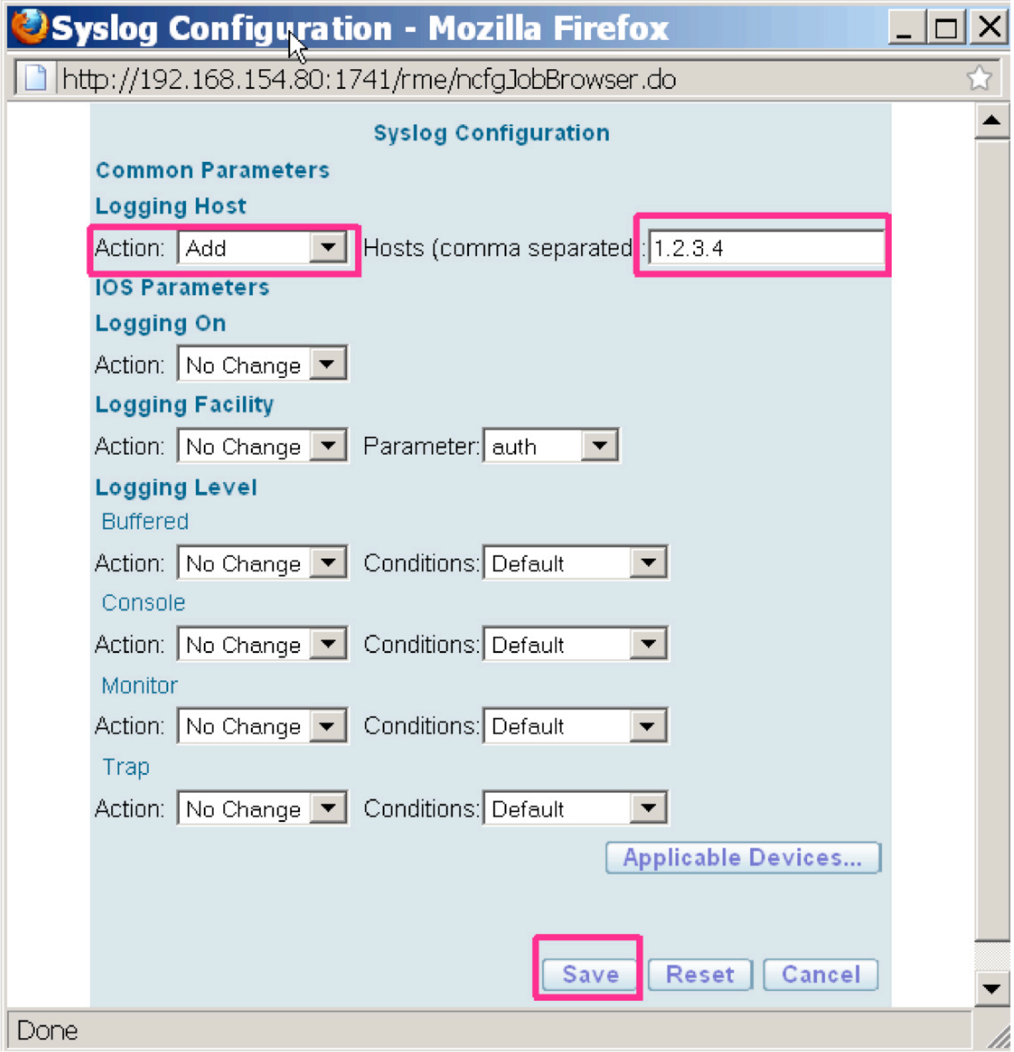


Figure 45. Syslog Configuration Window



Syslog Configuration - Mozilla Firefox

http://192.168.154.80:1741/rme/ncfgJobBrowser.do

Syslog Configuration

Common Parameters

Logging Host

Action: Add   Hosts (comma separated): 1.2.3.4

IOS Parameters

Logging On

Action: No Change

Logging Facility

Action: No Change   Parameter: auth

Logging Level

Buffered

Action: No Change   Conditions: Default

Console

Action: No Change   Conditions: Default

Monitor

Action: No Change   Conditions: Default

Trap

Action: No Change   Conditions: Default

Done

6. 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.

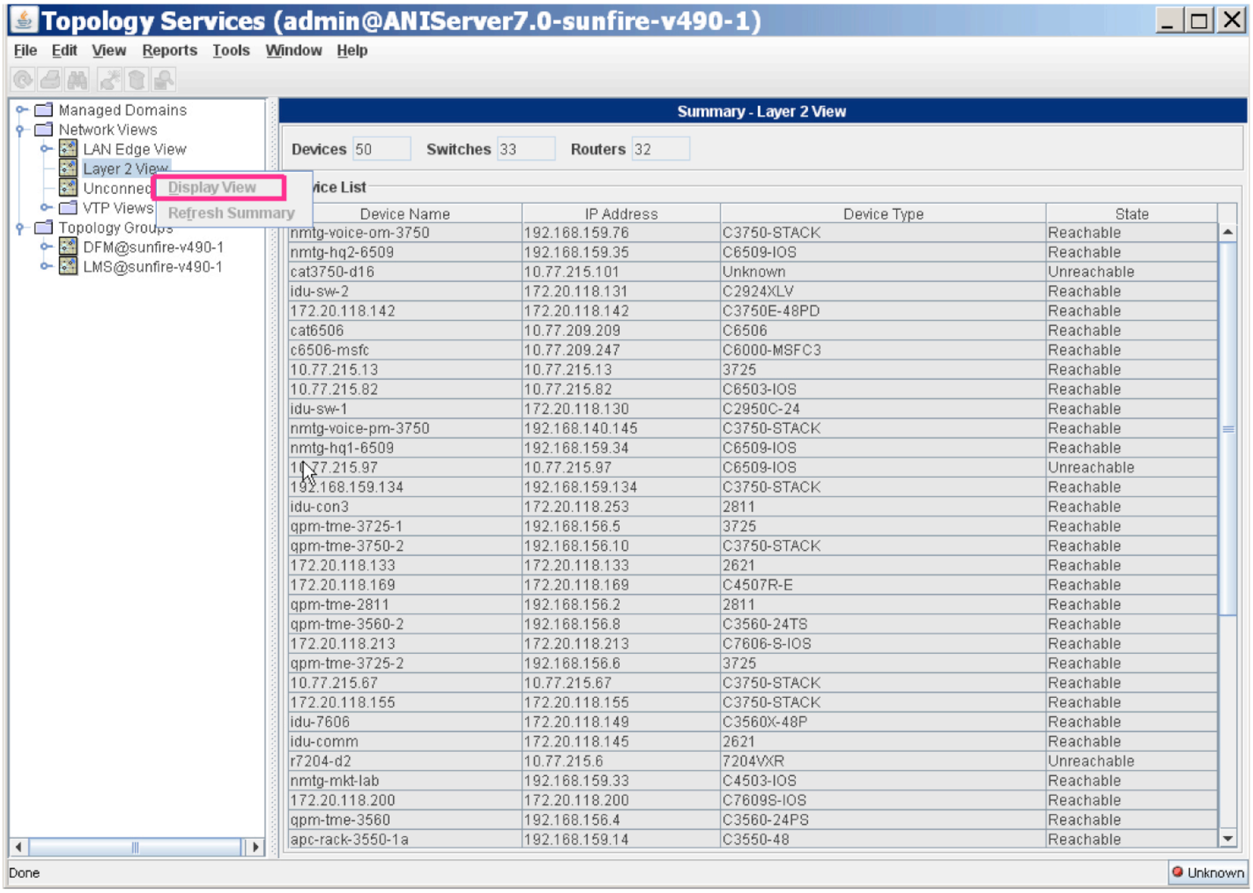
Topology

Topology Services is an application that enables you 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 (Figures 46 and 47).

Configuration → Topology

Figure 46. Topology Services Window



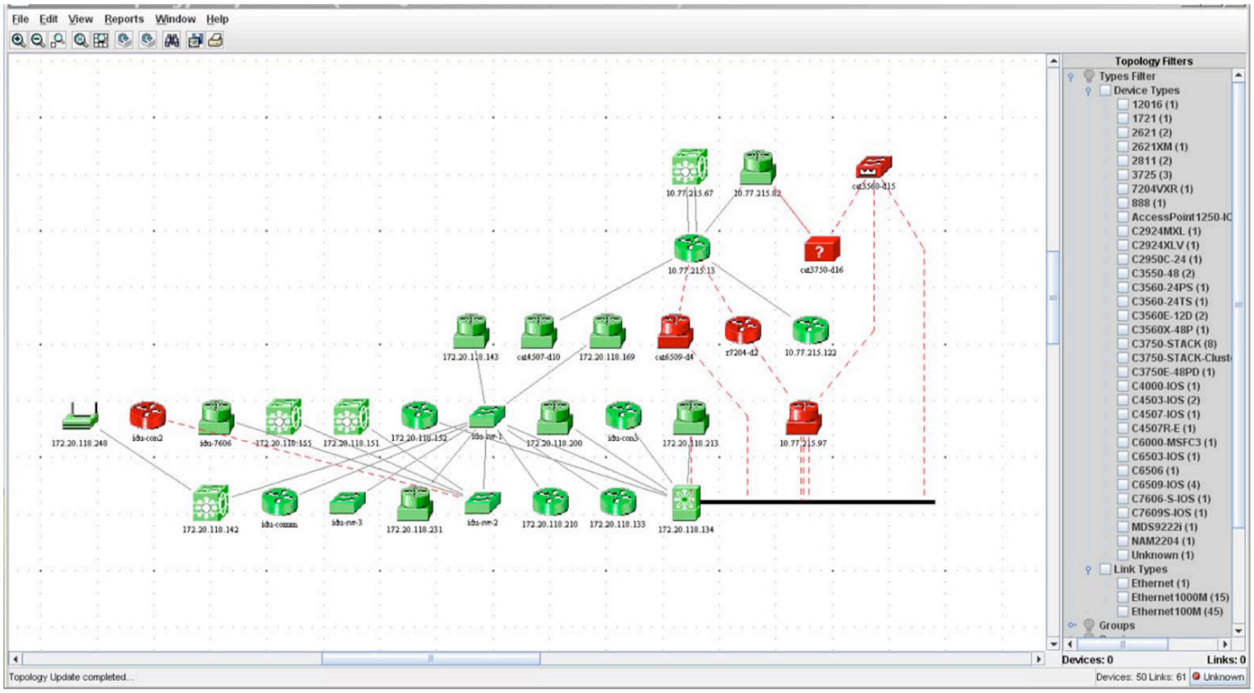
Summary - Layer 2 View

Devices 50 Switches 33 Routers 32

Device List

Device Name	IP Address	Device Type	State
nmtg-voice-om-3750	192.168.159.76	C3750-STACK	Reachable
nmtg-hq2-6509	192.168.159.35	C6509-IOS	Reachable
cat3750-d16	10.77.215.101	Unknown	Unreachable
idu-sw-2	172.20.118.131	C2924XLV	Reachable
172.20.118.142	172.20.118.142	C3750E-48PD	Reachable
cat6506	10.77.209.209	C6506	Reachable
c6506-msfc	10.77.209.247	C6000-MSFC3	Reachable
10.77.215.13	10.77.215.13	3725	Reachable
10.77.215.82	10.77.215.82	C6503-IOS	Reachable
idu-sw-1	172.20.118.130	C2950C-24	Reachable
nmtg-voice-pm-3750	192.168.140.145	C3750-STACK	Reachable
nmtg-hq1-6509	192.168.159.34	C6509-IOS	Reachable
10.77.215.97	10.77.215.97	C6509-IOS	Unreachable
192.168.159.134	192.168.159.134	C3750-STACK	Reachable
idu-con3	172.20.118.253	2811	Reachable
qpm-tme-3725-1	192.168.156.5	3725	Reachable
qpm-tme-3750-2	192.168.156.10	C3750-STACK	Reachable
172.20.118.133	172.20.118.133	2621	Reachable
172.20.118.169	172.20.118.169	C4507R-E	Reachable
qpm-tme-2811	192.168.156.2	2811	Reachable
qpm-tme-3560-2	192.168.156.8	C3560-24TS	Reachable
172.20.118.213	172.20.118.213	C7606-S-IOS	Reachable
qpm-tme-3725-2	192.168.156.6	3725	Reachable
10.77.215.67	10.77.215.67	C3750-STACK	Reachable
172.20.118.155	172.20.118.155	C3750-STACK	Reachable
idu-7606	172.20.118.149	C3560X-48P	Reachable
idu-comm	172.20.118.145	2621	Reachable
r7204-d2	10.77.215.6	7204VXR	Unreachable
nmtg-mkt-lab	192.168.159.33	C4503-IOS	Reachable
172.20.118.200	172.20.118.200	C7609S-IOS	Reachable
qpm-tme-3560	192.168.156.4	C3560-24PS	Reachable
apc-rack-3550-1a	192.168.159.14	C3550-48	Reachable

Figure 47. Topology Services Display View



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.

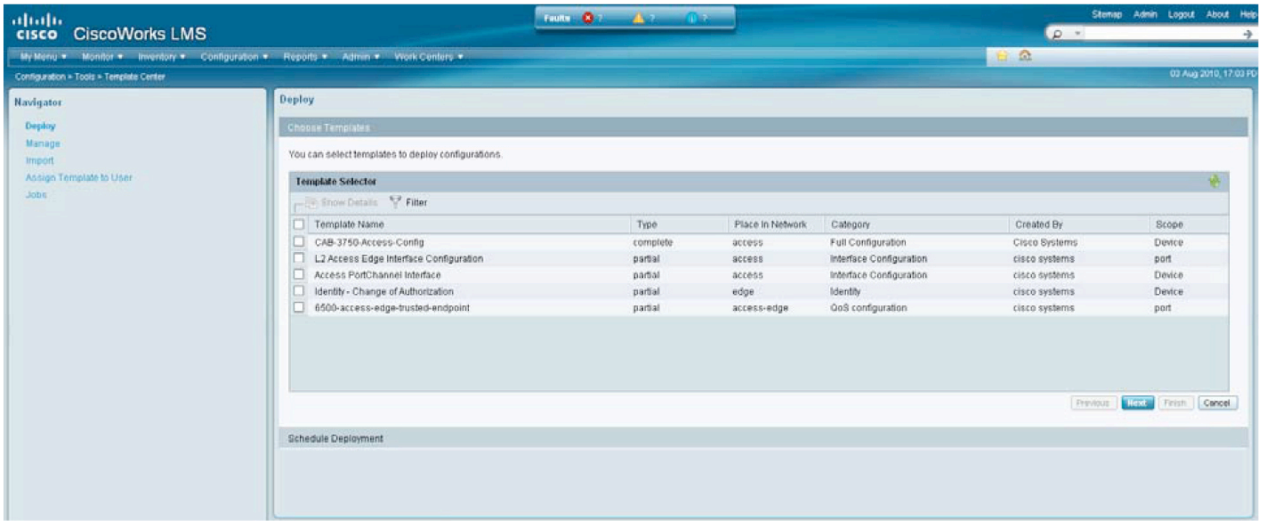
You can modify the system-defined templates and save the modified templates as user-defined templates. You can also import templates from a client machine, and these templates are stored as system-defined templates in LMS.

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

- L2 Access Edge Interface Configuration
- Access PortChannel Interface
- Identity-Change of Authorization
- CAB-3750-Access-Config
- 6500-access-edge-trusted-endpoint

To access the Template Center, go to **Configuration → Tools → Template Center** (Figure 48).

Figure 48. The Template Center



You can select templates to deploy configurations.

□	Template Name	Type	Place In Network	Category	Created By	Scope
□	CAB-3750-Access-Config	complete	access	Full Configuration	Cisco Systems	Device
□	L2 Access Edge Interface Configuration	partial	access	Interface Configuration	cisco systems	port
□	Access PortChannel Interface	partial	access	Interface Configuration	cisco systems	Device
□	Identity - Change of Authorization	partial	edge	Identity	cisco systems	Device
□	6500-access-edge-trusted-endpoint	partial	access-edge	QoS configuration	cisco systems	port

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.

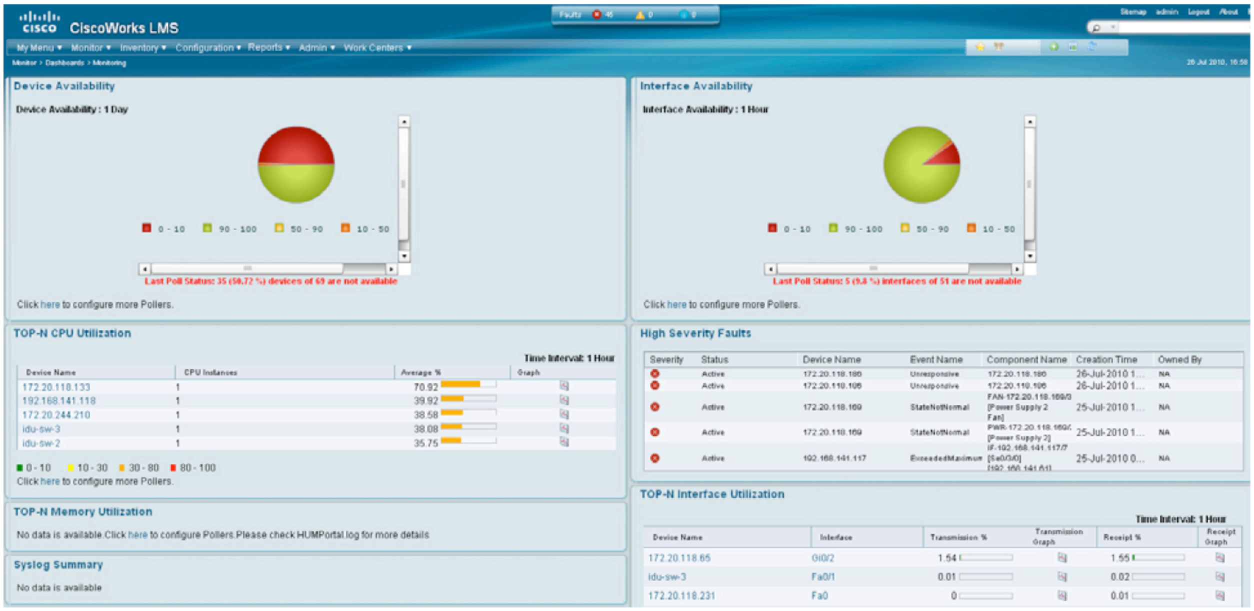
Job Management

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 49. Monitoring Dashboard


CiscoWorks LMS
Faults 46 0 0
Sitemap admin Logout About
My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾
Monitor > Dashboards > Monitoring
26 Jul 2010, 16:58
0 - 10
90 - 100
50 - 90
10 - 50
0 - 10
90 - 100
50 - 90
10 - 50
0 - 10
10 - 30
30 - 80
80 - 100

Device Availability

Device Availability : 1 Day

Last Poll Status: 35 (50.72 %) devices of 69 are not available

Click here to configure more Pollers.

Interface Availability

Interface Availability : 1 Hour

Last Poll Status: 5 (9.8 %) interfaces of 51 are not available

Click here to configure more Pollers.

TOP-N CPU Utilization

Time Interval: 1 Hour

Device Name	CPU Instances	Average %	Graph
172.20.118.133	1	70.92	
192.168.141.118	1	39.92	
172.20.244.210	1	38.58	
idu-sw-3	1	38.08	
idu-sw-2	1	35.75	

Click here to configure more Pollers.

High Severity Faults

Severity	Status	Device Name	Event Name	Component Name	Creation Time	Owned By
●	Active	172.20.118.186	Unresponsive	172.20.118.186	26-Jul-2010 1...	NA
●	Active	172.20.110.106	Unresponsive	172.20.110.106	26-Jul-2010 1...	NA
●	Active	172.20.118.169	StateNotNormal	FAN-172.20.118.169/3 [Power Supply 2 Fan]	25-Jul-2010 1...	NA
●	Active	172.20.110.169	StateNotNormal	PWR-172.20.118.169/ [Power Supply 2]	25-Jul-2010 1...	NA
●	Active	192.168.141.117	ExceededMaximum	IF-192.168.141.117/7 [Se0/3/0] [192.168.141.61]	25-Jul-2010 0...	NA

TOP-N Memory Utilization

No data is available.Click here to configure Pollers.Please check HUMPortal.log for more details

TOP-N Interface Utilization

Time Interval: 1 Hour

Device Name	Interface	Transmission %	Transmission Graph	Receipt %	Receipt Graph
172.20.118.65	Gi0/2	1.54		1.55	
idu-sw-3	Fa0/1	0.01		0.02	
172.20.118.231	Fa0	0		0.01	

Syslog Summary

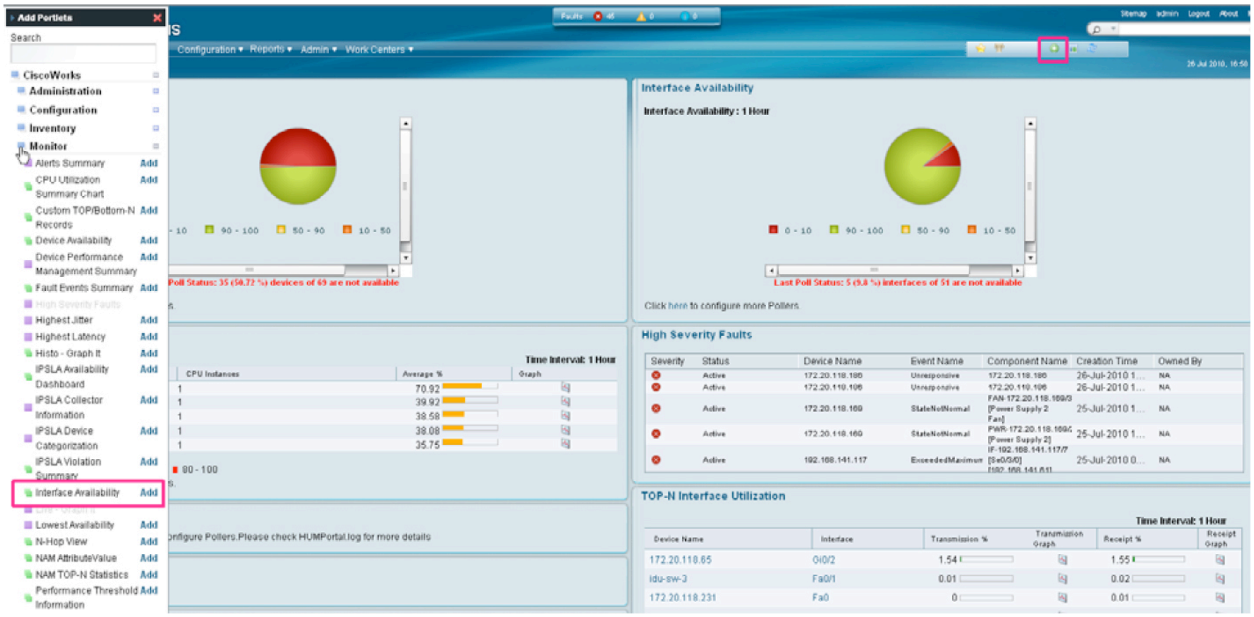
No data is available

Customizing Monitoring Dashboard

Adding a Portlet

Click the Add Portlet icon in Figure 49 to get the list of portlets. Choose a portlet, for example, Interface Availability to add that portlet (Figure 50).

Figure 50. Checking on Interface Availability



Poll Status: 35 (50.72 %) devices of 69 are not available

Time Interval: 1 Hour

CPU Instances	Average %	Graph
1	70.92	
1	39.92	
1	38.58	
1	38.08	
1	35.75	

onfigure Pollers.Please check HUMPortal.log for more details

Last Poll Status: 5 (9.8 %) interfaces of 51 are not available

Click here to configure more Pollers.

High Severity Faults

Severity	Status	Device Name	Event Name	Component Name	Creation Time	Owned By
●	Active	172.20.118.186	Unresponsive	172.20.118.186	26-Jul-2010 1...	NA
●	Active	172.20.110.106	Unresponsive	172.20.110.106	26-Jul-2010 1...	NA
●	Active	172.20.118.169	StateNotNormal	FAN-172.20.118.169/3 [Power Supply 2 Fan]	25-Jul-2010 1...	NA
●	Active	172.20.118.169	StateNotNormal	PWR-172.20.118.169/ [Power Supply 2]	25-Jul-2010 1...	NA
●	Active	192.168.141.117	ExceededMaximum	IF-192.168.141.117/7 [Se0/3/0] [192.168.141.61]	25-Jul-2010 0...	NA

TOP-N Interface Utilization

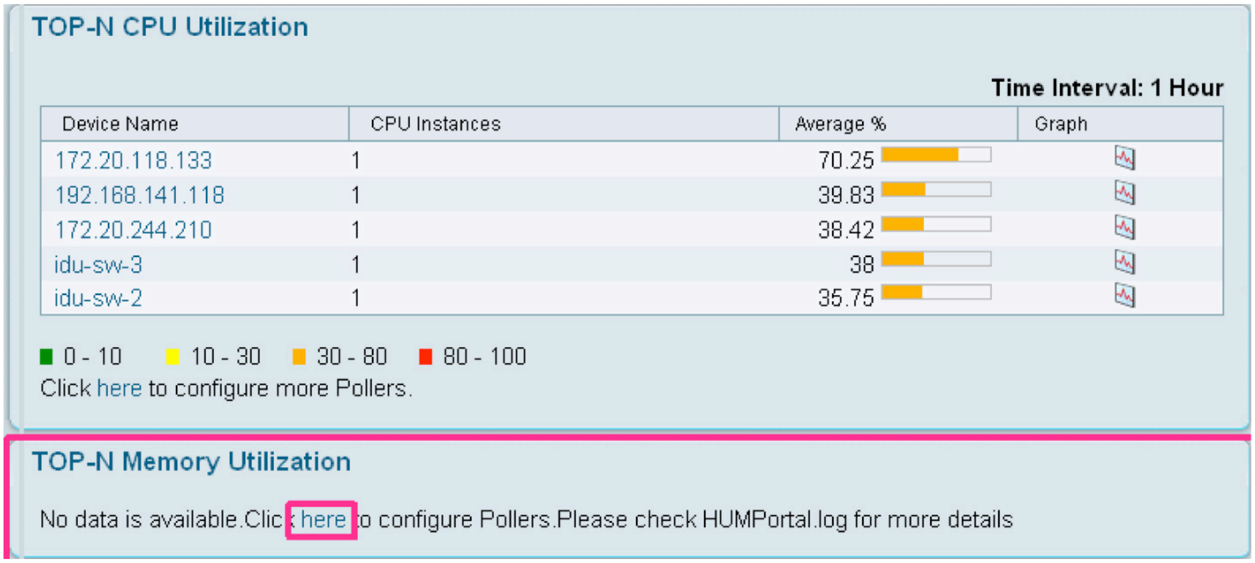
Time Interval: 1 Hour

Device Name	Interface	Transmission %	Transmission Graph	Receipt %	Receipt Graph
172.20.118.65	Gi0/2	1.54		1.55	
idu-sw-3	Fa0/1	0.01		0.02	
172.20.118.231	Fa0	0		0.01	

Adding Contents to a 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. See Figure 51.

Figure 51. Top-N Memory Utilization



TOP-N CPU Utilization

Time Interval: 1 Hour

Device Name	CPU Instances	Average %	Graph
172.20.118.133	1	70.25	
192.168.141.118	1	39.83	
172.20.244.210	1	38.42	
idu-sw-3	1	38	
idu-sw-2	1	35.75	

🟩 0 - 10 🟨 10 - 30 🟧 30 - 80 🟥 80 - 100

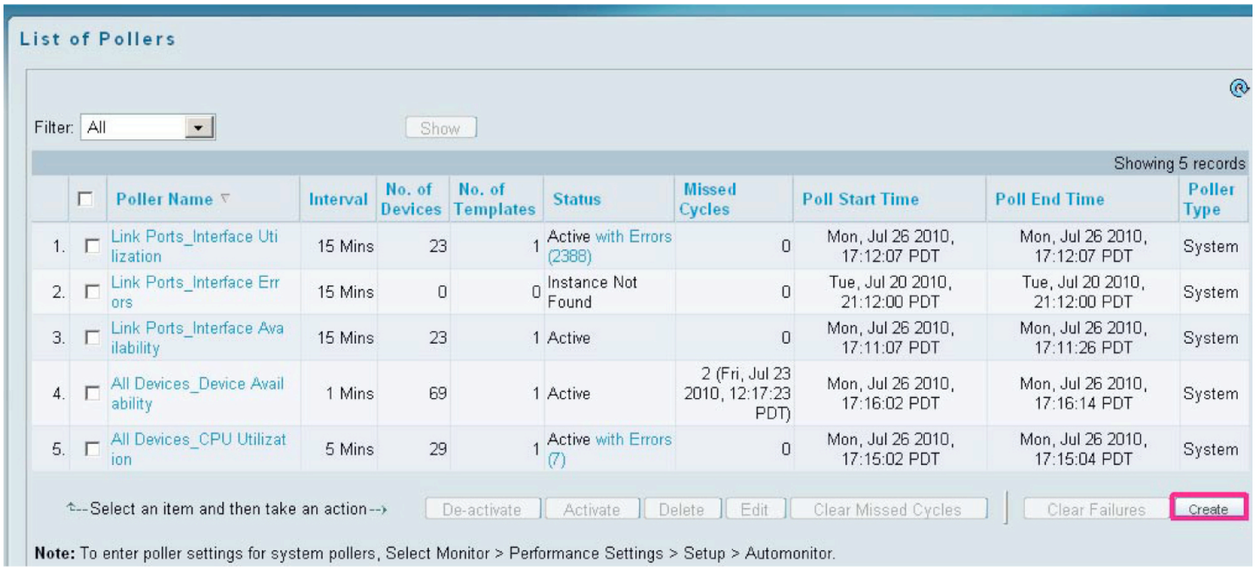
Click here to configure more Pollers.

TOP-N Memory Utilization

No data is available.Click here to configure Pollers.Please check HUMPortal.log for more details

Click the link **here** 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 52 and 53.

Figure 52. List of Pollers



List of Pollers

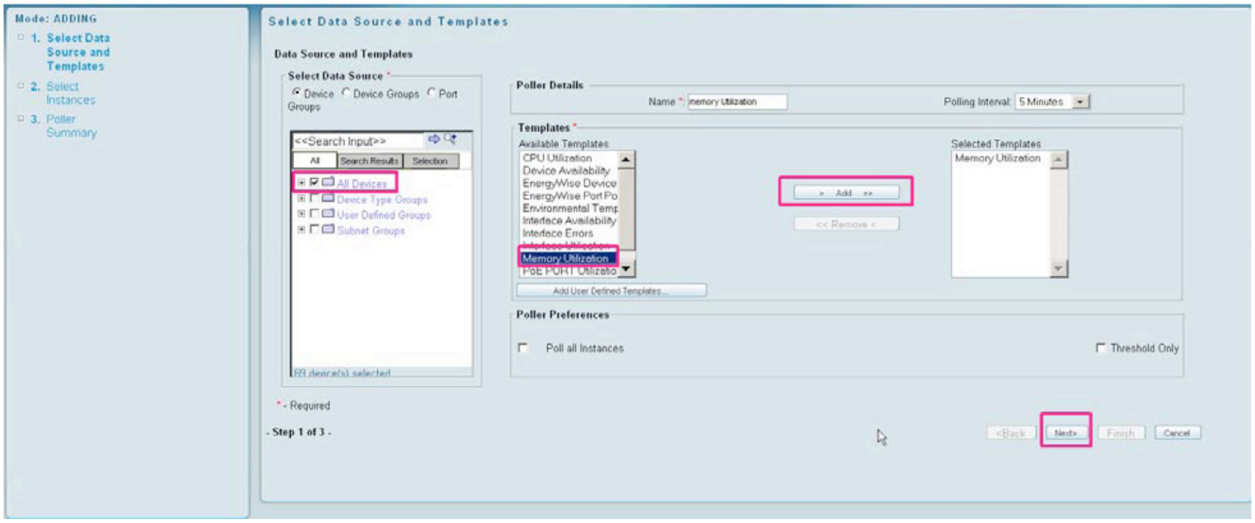
Filter: All

Showing 5 records

	□	Poller Name	Interval	No. of Devices	No. of Templates	Status	Missed Cycles	Poll Start Time	Poll End Time	Poller Type
1.	□	Link Ports_Interface Utilization	15 Mins	23	1	Active with Errors (2388)	0	Mon, Jul 26 2010, 17:12:07 PDT	Mon, Jul 26 2010, 17:12:07 PDT	System
2.	□	Link Ports_Interface Errors	15 Mins	0	0	Instance Not Found	0	Tue, Jul 20 2010, 21:12:00 PDT	Tue, Jul 20 2010, 21:12:00 PDT	System
3.	□	Link Ports_Interface Availability	15 Mins	23	1	Active	0	Mon, Jul 26 2010, 17:11:07 PDT	Mon, Jul 26 2010, 17:11:26 PDT	System
4.	□	All Devices_Device Availability	1 Mins	69	1	Active	2 (Fri, Jul 23 2010, 12:17:23 PDT)	Mon, Jul 26 2010, 17:16:02 PDT	Mon, Jul 26 2010, 17:16:14 PDT	System
5.	□	All Devices_CPU Utilization	5 Mins	29	1	Active with Errors (7)	0	Mon, Jul 26 2010, 17:15:02 PDT	Mon, Jul 26 2010, 17:15:04 PDT	System

Note: To enter poller settings for system pollers, Select Monitor > Performance Settings > Setup > Automonitor.

Figure 53. Selecting the Data Source and Templates



Mode: ADDING

1. Select Data Source and Templates
2. Select Instances
3. Poller Summary

Select Data Source and Templates

Data Source and Templates

Select Data Source *: ● Device ○ Device Groups ○ Port Groups

☑ All Devices

69 device(s) selected

Poller Details

Name *: memory Utilization

Polling Interval: 5 Minutes

Templates *

Available Templates: CPU Utilization, Device Availability, EnergyWise Device, EnergyWise Port Po, Environmental Temp, Interface Availability, Interface Errors, Interface Utilization, Memory Utilization, PoE PORT Utilizatio

Selected Templates: Memory Utilization

Poller Preferences

□ Poll all Instances

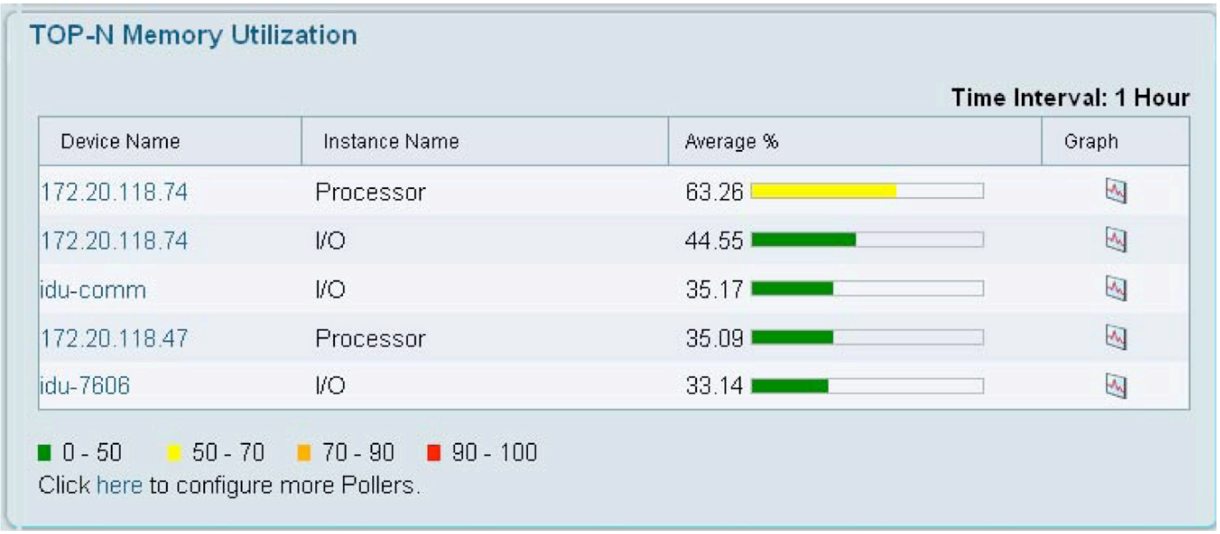
□ Threshold Only

* - Required

- Step 1 of 3 -

Once the poller is created the portlet will be populated with the Top-N memory utilization data (Figure 54).

Figure 54. Top-N Memory Utilization



TOP-N Memory Utilization

Time Interval: 1 Hour

Device Name	Instance Name	Average %	Graph
172.20.118.74	Processor	63.26	📈
172.20.118.74	I/O	44.55	📈
idu-comm	I/O	35.17	📈
172.20.118.47	Processor	35.09	📈
idu-7606	I/O	33.14	📈

🟩 0 - 50 🟨 50 - 70 🟧 70 - 90 🟥 90 - 100

Click here to configure more Pollers.

Fault Management

Business Scenarios

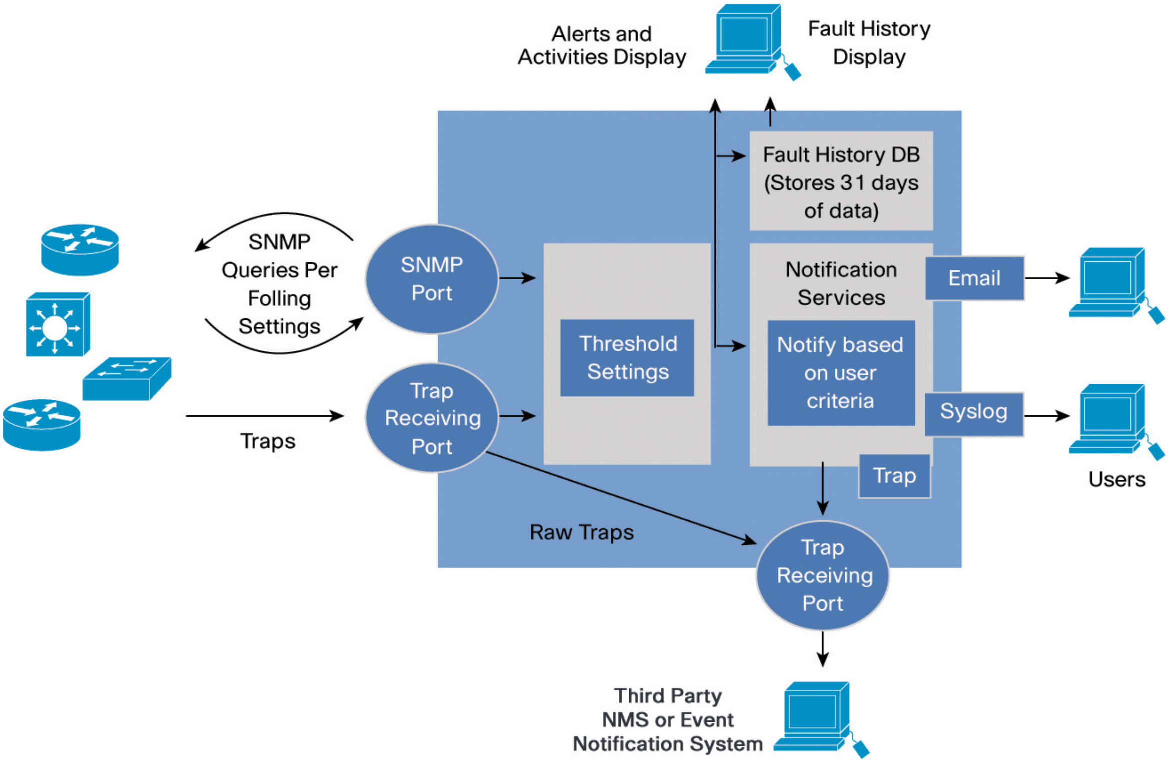
On a daily basis, network administrators face many challenges to maintain a healthy running network to support business needs. They constantly ask questions like:

- 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?

CiscoWorks 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.

Fault Management Architecture

Figure 55. Fault Management


Alerts and Activities Display
Fault History Display
Fault History DB (Stores 31 days of data)
SNMP Queries Per Folling Settings
SNMP Port
Notification Services
Email
Threshold Settings
Notify based on user criteria
Trap Receiving Port
Syslog
Traps
Trap
Users
Raw Traps
Trap Receiving Port
Third Party NMS or Event Notification System

CiscoWorks uses SNMP polling and SNMP traps to discover and display real-time faults. See Figure 55. 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.

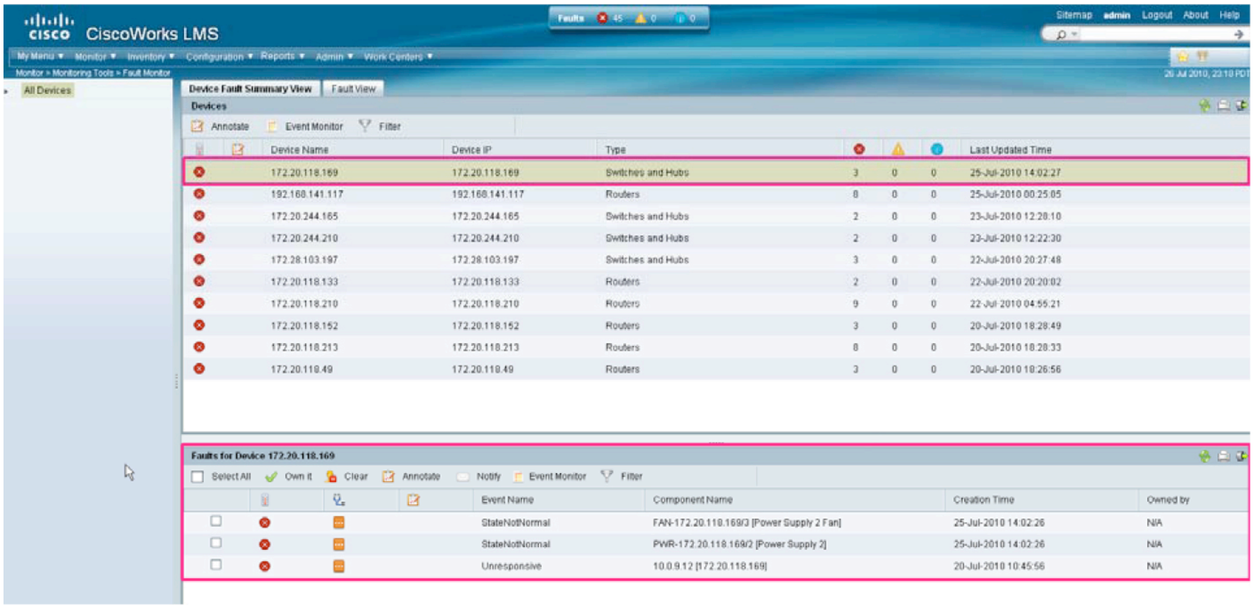
An event refers to the activities or changes happening in the network. Examples for events are Config Change, user login, user logout, and so on.

Fault Monitor collects information on faults and events from all devices in real time 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 56. The Fault Monitor Device Fault Sumary


CiscoWorks LMS
Faults 45 0 0
Sitemap admin Logout About Help
My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾
Monitor » Monitoring Tools » Fault Monitor
26 Jul 2010, 23:18 PDT
All Devices
Device Fault Summary View
Fault View
Devices
Annotate
Event Monitor
Filter

	Device Name	Device IP	Type	⊗	⚠	●	Last Updated Time
⊗	172.20.118.169	172.20.118.169	Switches and Hubs	3	0	0	25-Jul-2010 14:02:27
⊗	192.168.141.117	192.168.141.117	Routers	8	0	0	25-Jul-2010 00:25:05
⊗	172.20.244.165	172.20.244.165	Switches and Hubs	2	0	0	23-Jul-2010 12:28:10
⊗	172.20.244.210	172.20.244.210	Switches and Hubs	2	0	0	23-Jul-2010 12:22:30
⊗	172.28.103.197	172.28.103.197	Switches and Hubs	3	0	0	22-Jul-2010 20:27:48
⊗	172.20.118.133	172.20.118.133	Routers	2	0	0	22-Jul-2010 20:20:02
⊗	172.20.118.210	172.20.118.210	Routers	9	0	0	22-Jul-2010 04:55:21
⊗	172.20.118.152	172.20.118.152	Routers	3	0	0	20-Jul-2010 18:28:49
⊗	172.20.118.213	172.20.118.213	Routers	8	0	0	20-Jul-2010 18:28:33
⊗	172.20.118.49	172.20.118.49	Routers	3	0	0	20-Jul-2010 18:26:56

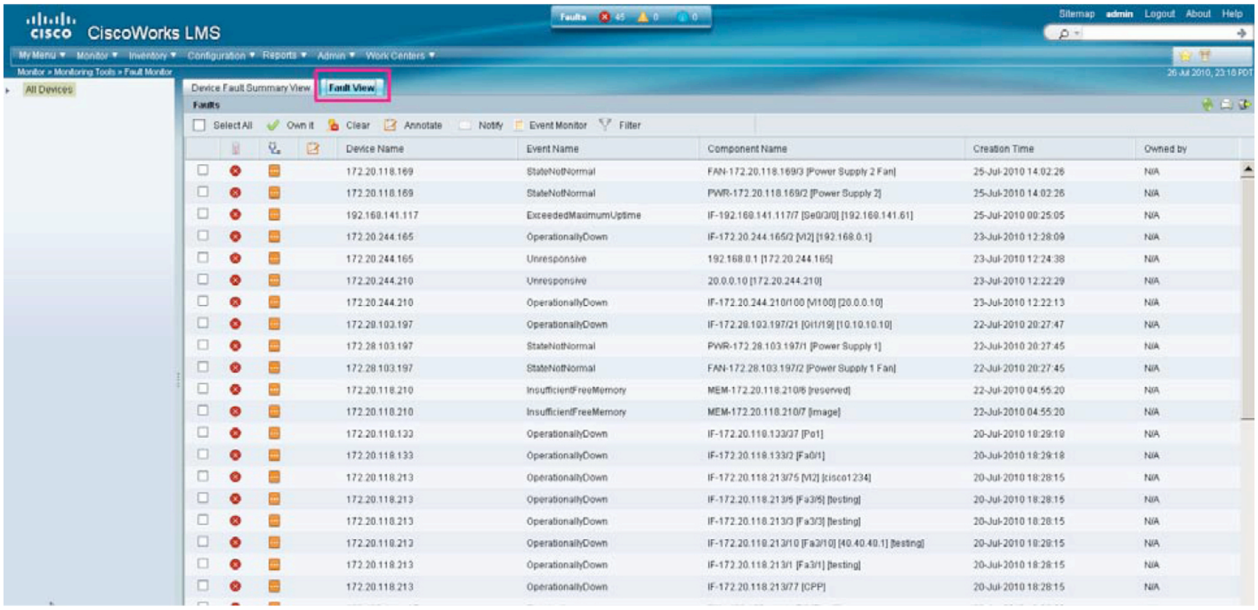
Faults for Device 172.20.118.169

		Event Name	Component Name	Creation Time	Owned by
□	⊗	StateNotNormal	FAN-172.20.118.169/3 [Power Supply 2 Fan]	25-Jul-2010 14:02:26	N/A
□	⊗	StateNotNormal	PWR-172.20.118.169/2 [Power Supply 2]	25-Jul-2010 14:02:26	N/A
□	⊗	Unresponsive	10.0.9.12 [172.20.118.169]	20-Jul-2010 10:45:56	N/A

In Figure 56, the top portion shows the devices. By clicking on 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 57).

Figure 57. The Fault View Tab


CiscoWorks LMS
Faults 45 0 0
Sitemap admin Logout About Help
My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾
Monitor » Monitoring Tools » Fault Monitor
26 Jul 2010, 23:18 PDT
All Devices
Device Fault Summary View
Fault View
Faults
□ Select All
Own it
Clear
Annotate
Notify
Event Monitor
Filter

		Device Name	Event Name	Component Name	Creation Time	Owned by
□	⊗	172.20.118.169	StateNotNormal	FAN-172.20.118.169/3 [Power Supply 2 Fan]	25-Jul-2010 14:02:26	N/A
□	⊗	172.20.118.169	StateNotNormal	PWR-172.20.118.169/2 [Power Supply 2]	25-Jul-2010 14:02:26	N/A
□	⊗	192.168.141.117	ExceededMaximumUptime	IF-192.168.141.117/7 [Se0/3/0] [192.168.141.61]	25-Jul-2010 00:25:05	N/A
□	⊗	172.20.244.165	OperationallyDown	IF-172.20.244.165/2 [M2] [192.168.0.1]	23-Jul-2010 12:28:09	N/A
□	⊗	172.20.244.165	Unresponsive	192.168.0.1 [172.20.244.165]	23-Jul-2010 12:24:38	N/A
□	⊗	172.20.244.210	Unresponsive	20.0.0.10 [172.20.244.210]	23-Jul-2010 12:22:29	N/A
□	⊗	172.20.244.210	OperationallyDown	IF-172.20.244.210/100 [M100] [20.0.0.10]	23-Jul-2010 12:22:13	N/A
□	⊗	172.28.103.197	OperationallyDown	IF-172.28.103.197/21 [Gi1/19] [10.10.10.10]	22-Jul-2010 20:27:47	N/A
□	⊗	172.28.103.197	StateNotNormal	PWR-172.28.103.197/1 [Power Supply 1]	22-Jul-2010 20:27:45	N/A
□	⊗	172.28.103.197	StateNotNormal	FAN-172.28.103.197/2 [Power Supply 1 Fan]	22-Jul-2010 20:27:45	N/A
□	⊗	172.20.118.210	InsufficientFreeMemory	MEM-172.20.118.210/6 [reserved]	22-Jul-2010 04:55:20	N/A
□	⊗	172.20.118.210	InsufficientFreeMemory	MEM-172.20.118.210/7 [image]	22-Jul-2010 04:55:20	N/A
□	⊗	172.20.118.133	OperationallyDown	IF-172.20.118.133/37 [Po1]	20-Jul-2010 18:29:18	N/A
□	⊗	172.20.118.133	OperationallyDown	IF-172.20.118.133/2 [Fa0/1]	20-Jul-2010 18:29:18	N/A
□	⊗	172.20.118.213	OperationallyDown	IF-172.20.118.213/75 [M2] [cisco1234]	20-Jul-2010 18:28:15	N/A
□	⊗	172.20.118.213	OperationallyDown	IF-172.20.118.213/5 [Fa3/5] [testing]	20-Jul-2010 18:28:15	N/A
□	⊗	172.20.118.213	OperationallyDown	IF-172.20.118.213/3 [Fa3/3] [testing]	20-Jul-2010 18:28:15	N/A
□	⊗	172.20.118.213	OperationallyDown	IF-172.20.118.213/10 [Fa3/10] [40.40.40.1] [testing]	20-Jul-2010 18:28:15	N/A
□	⊗	172.20.118.213	OperationallyDown	IF-172.20.118.213/1 [Fa3/1] [testing]	20-Jul-2010 18:28:15	N/A
□	⊗	172.20.118.213	OperationallyDown	IF-172.20.118.213/77 [CPP]	20-Jul-2010 18:28:15	N/A

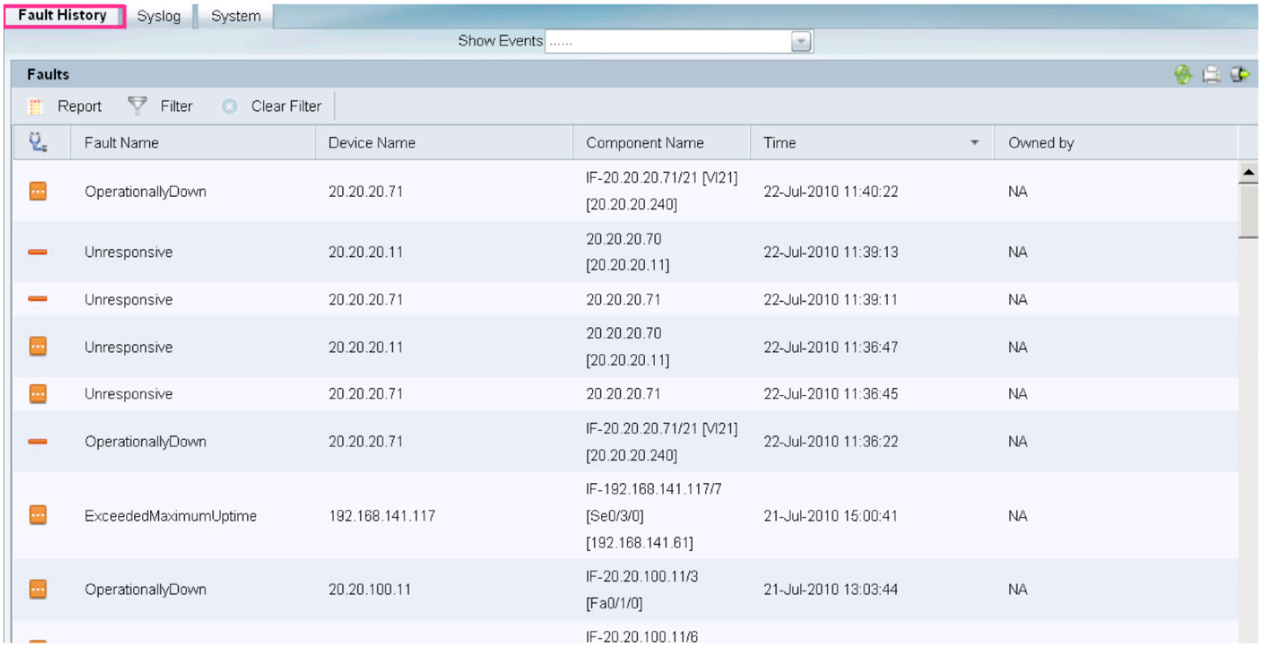
In this window, you can Clear, Own, Notify, or Annotate an event.

- **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 Figure 58).

Figure 58. Fault History



	Fault Name	Device Name	Component Name	Time	Owned by
■	OperationallyDown	20.20.20.71	IF-20.20.20.71/21 [Vl21] [20.20.20.240]	22-Jul-2010 11:40:22	NA
▬	Unresponsive	20.20.20.11	20.20.20.70 [20.20.20.11]	22-Jul-2010 11:39:13	NA
▬	Unresponsive	20.20.20.71	20.20.20.71	22-Jul-2010 11:39:11	NA
■	Unresponsive	20.20.20.11	20.20.20.70 [20.20.20.11]	22-Jul-2010 11:36:47	NA
■	Unresponsive	20.20.20.71	20.20.20.71	22-Jul-2010 11:36:45	NA
▬	OperationallyDown	20.20.20.71	IF-20.20.20.71/21 [Vl21] [20.20.20.240]	22-Jul-2010 11:36:22	NA
■	ExceededMaximumUptime	192.168.141.117	IF-192.168.141.117/7 [Se0/3/0] [192.168.141.61]	21-Jul-2010 15:00:41	NA
■	OperationallyDown	20.20.100.11	IF-20.20.100.11/3 [Fa0/1/0]	21-Jul-2010 13:03:44	NA
■			IF-20.20.100.11/6		

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 network but 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.

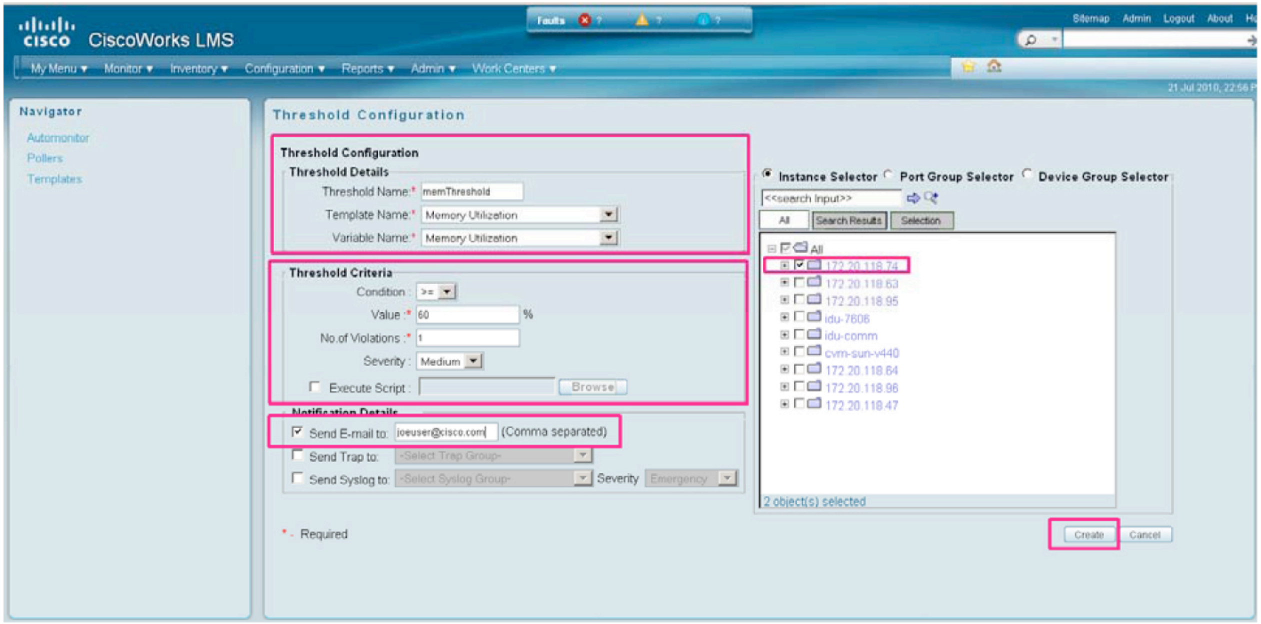
CiscoWorks LMS provides organizations with:

- CPU, memory, Interface/port monitoring for utilization and availability levels
- Support for system-defined MIB templates that enable easy 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** (Figure 59).

Figure 59. Thresholds and Notifications



Threshold Configuration

Threshold Configuration

Threshold Details

Threshold Name:* memThreshold

Template Name:* Memory Utilization

Variable Name:* Memory Utilization

Threshold Criteria

Condition : >=

Value :* 60 %

No.of Violations :* 1

Severity : Medium

□ Execute Script :

Notification Details

☑ Send E-mail to: joeuser@cisco.com (Comma separated)

□ Send Trap to: -Select Trap Group-

□ Send Syslog to: -Select Syslog Group- Severity Emergency

* - Required

● Instance Selector ○ Port Group Selector ○ Device Group Selector

<<search Input>>

- ☑ All
  - ☑ 172.20.118.74
  - □ 172.20.118.63
  - □ 172.20.118.95
  - □ idu-7606
  - □ idu-comm
  - □ cvm-sun-v440
  - □ 172.20.118.64
  - □ 172.20.118.96
  - □ 172.20.118.47

2 object(s) selected

Workflow for Creating a Threshold

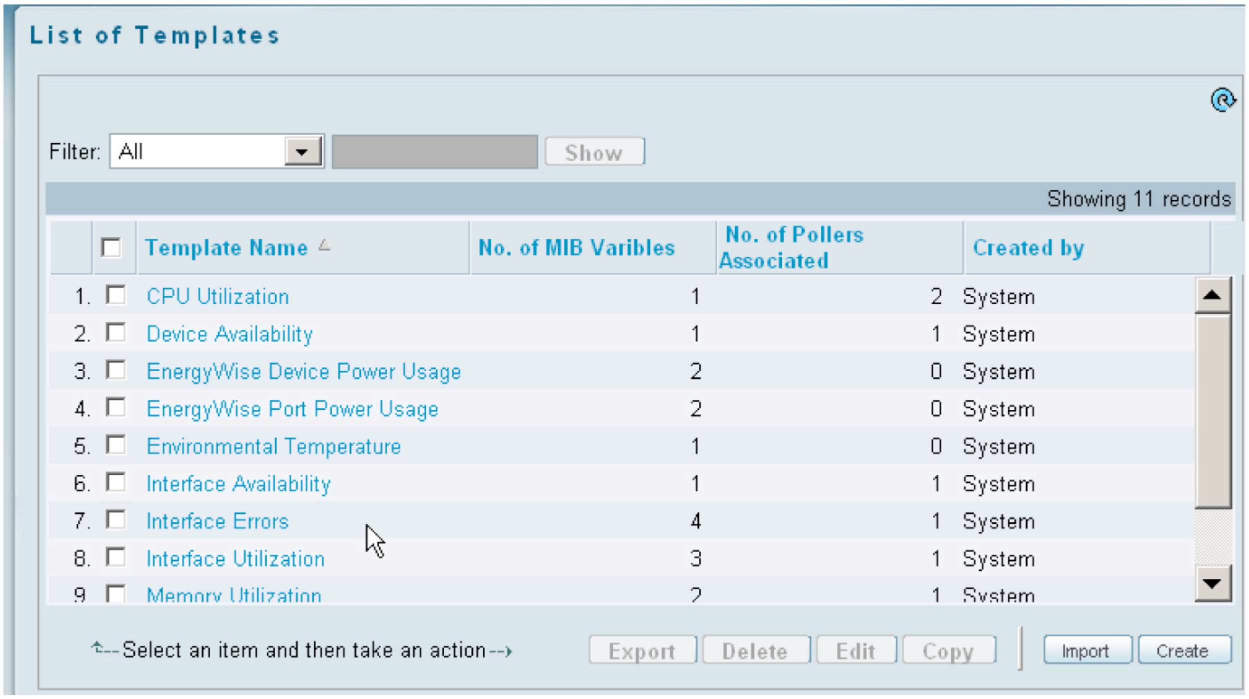
- Choose the variable from the template that you need to set the threshold on.
- Define the condition: threshold value, severity.
- Define the action-email, trap, or syslog generation-if the threshold condition occurs.
- Choose the device where you want to monitor this threshold.

Understand the Templates

System-defined templates are logical groups of MIB objects users want to poll. LMS has available the system-defined templates shown in Figure 60.

Monitor → **Performance Settings** → Setup → Templates

Figure 60. System-Defined Templates



	□	Template Name	No. of MIB Varibles	No. of Pollers Associated	Created by
1.	□	CPU Utilization	1	2	System
2.	□	Device Availability	1	1	System
3.	□	EnergyWise Device Power Usage	2	0	System
4.	□	EnergyWise Port Power Usage	2	0	System
5.	□	Environmental Temperature	1	0	System
6.	□	Interface Availability	1	1	System
7.	□	Interface Errors	4	1	System
8.	□	Interface Utilization	3	1	System
9	□	Memory Utilization	2	1	System

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

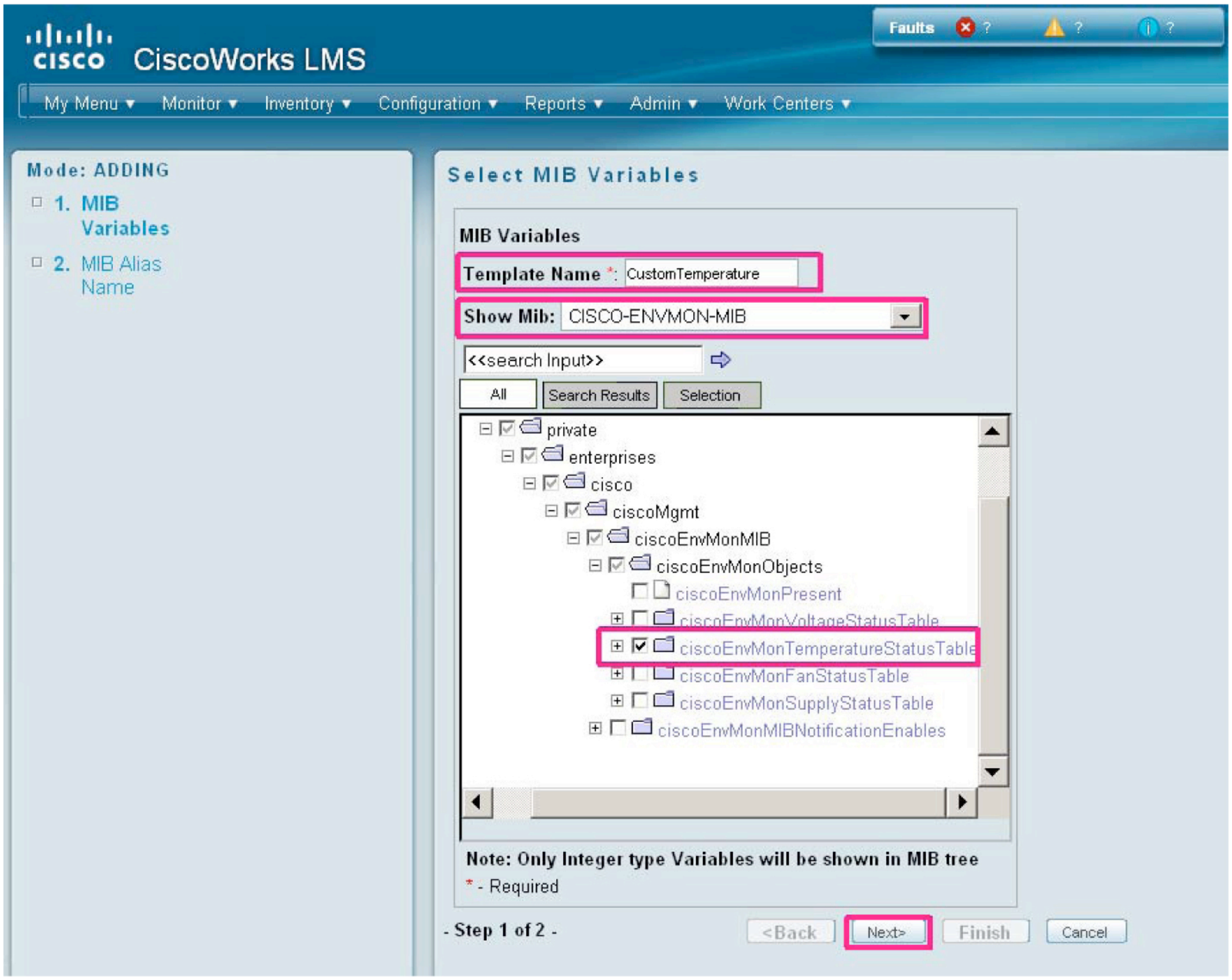
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENVMON-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PROCESS-MIB
- ENTITY-MIB
- OLD-CISCO-CHASSIS-MIB
- RFC1213-MIB
- IF-MIB
- CISCO-POWER-EHTHERNET-EXT-MIB
- POWER-EHTHERNET-MIB
- CISCO-RTTMON-MIB

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**.

For example, in Figure 61 we create a template to poll the temperature MIB objects using the CISCO-ENVMON-MIB.

Figure 61. User-Defined Template



Template Name *: CustomTemperature

Show Mib: CISCO-ENVMON-MIB

<<search Input>>
All
Search Results
Selection
private
enterprises
cisco
ciscoMgmt
ciscoEnvMonMIB
ciscoEnvMonObjects
ciscoEnvMonPresent
ciscoEnvMonVoltageStatusTable
ciscoEnvMonTemperatureStatusTable
ciscoEnvMonFanStatusTable
ciscoEnvMonSupplyStatusTable
ciscoEnvMonMIBNotificationEnables

Note: Only Integer type Variables will be shown in MIB tree

* - Required

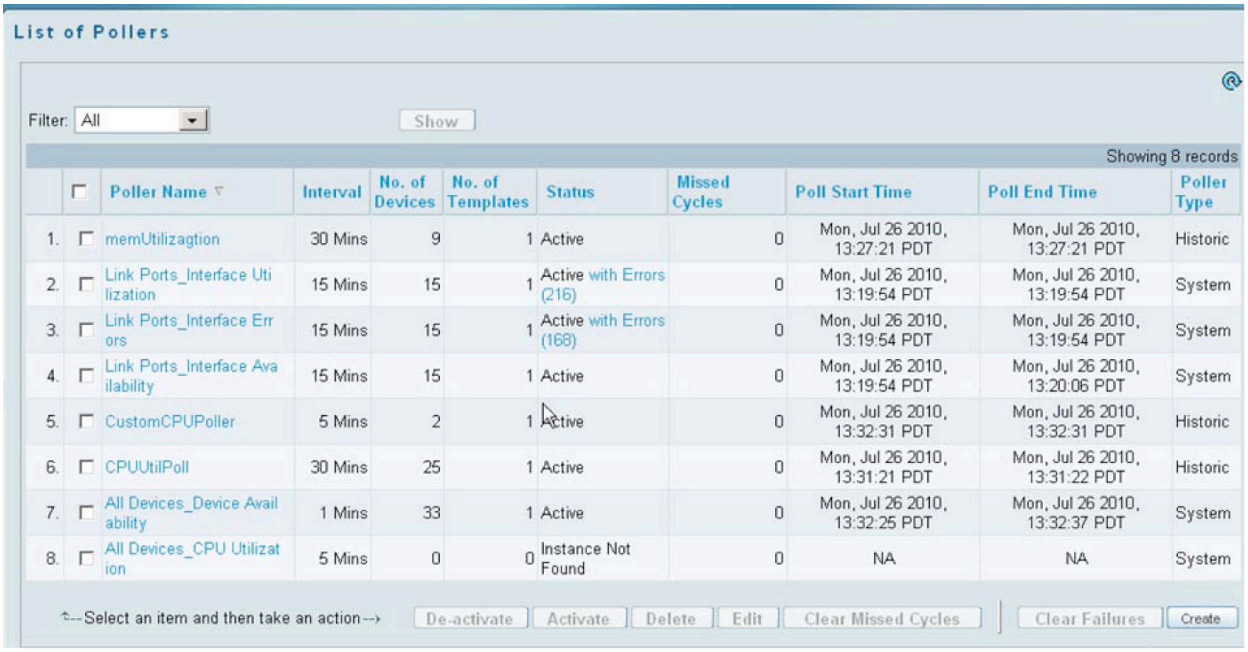
- Step 1 of 2 -

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 62.

Monitor → **Performance Settings** → Setup → Pollers

Figure 62. List of Pollers



List of Pollers

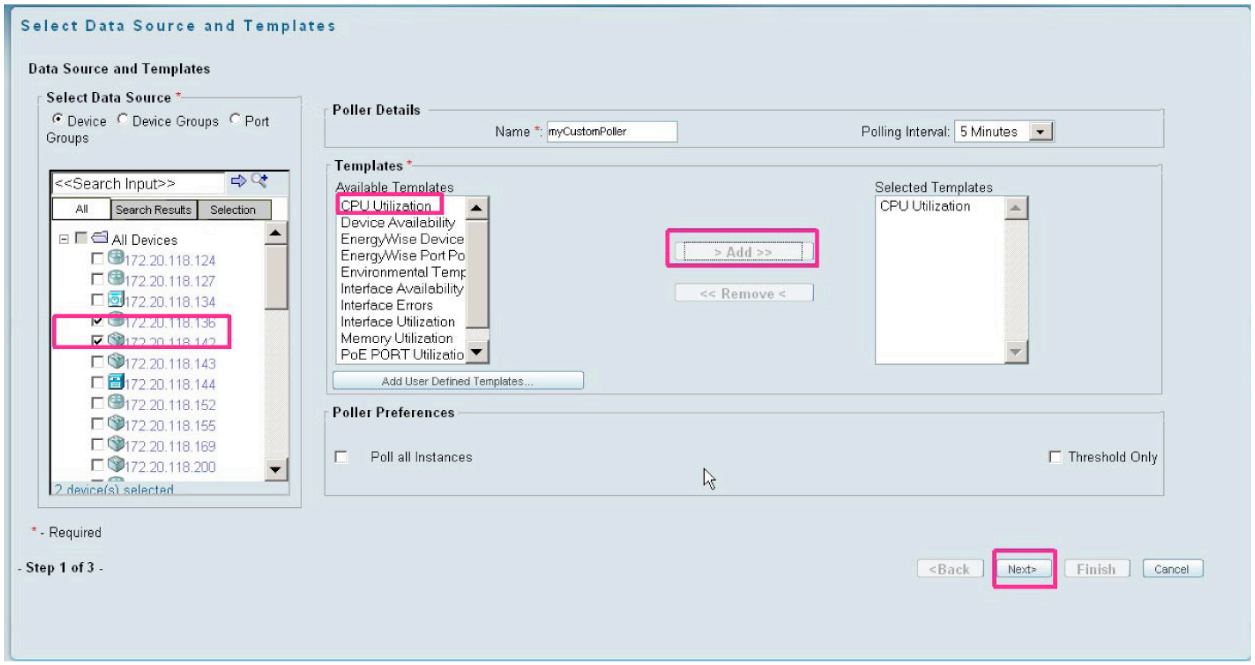
Filter: All

Showing 8 records

	☐	Poller Name	Interval	No. of Devices	No. of Templates	Status	Missed Cycles	Poll Start Time	Poll End Time	Poller Type
1.	☐	memUtilizagtion	30 Mins	9	1	Active	0	Mon, Jul 26 2010, 13:27:21 PDT	Mon, Jul 26 2010, 13:27:21 PDT	Historic
2.	☐	Link Ports_Interface Utilization	15 Mins	15	1	Active with Errors (216)	0	Mon, Jul 26 2010, 13:19:54 PDT	Mon, Jul 26 2010, 13:19:54 PDT	System
3.	☐	Link Ports_Interface Errors	15 Mins	15	1	Active with Errors (168)	0	Mon, Jul 26 2010, 13:19:54 PDT	Mon, Jul 26 2010, 13:19:54 PDT	System
4.	☐	Link Ports_Interface Availability	15 Mins	15	1	Active	0	Mon, Jul 26 2010, 13:19:54 PDT	Mon, Jul 26 2010, 13:20:06 PDT	System
5.	☐	CustomCPUPoller	5 Mins	2	1	Active	0	Mon, Jul 26 2010, 13:32:31 PDT	Mon, Jul 26 2010, 13:32:31 PDT	Historic
6.	☐	CPUUtilPoll	30 Mins	25	1	Active	0	Mon, Jul 26 2010, 13:31:21 PDT	Mon, Jul 26 2010, 13:31:22 PDT	Historic
7.	☐	All Devices_Device Availability	1 Mins	33	1	Active	0	Mon, Jul 26 2010, 13:32:25 PDT	Mon, Jul 26 2010, 13:32:37 PDT	System
8.	☐	All Devices_CPU Utilization	5 Mins	0	0	Instance Not Found	0	NA	NA	System

In Figure 63, we create a poller, myCustomPoller, which polls the selected two devices using the system-defined template-CPU Utilization. The setup options include poller name, devices, template, and polling interval.

Figure 63. Creating a Custom Poller



Select Data Source and Templates

Data Source and Templates

Select Data Source *

● Device ○ Device Groups ○ Port Groups

<<Search Input>>

All | Search Results | Selection

⊟ ☐ All Devices
- ☐ 172.20.118.124
- ☐ 172.20.118.127
- ☐ 172.20.118.134
- ☑ 172.20.118.136
- ☑ 172.20.118.142
- ☐ 172.20.118.143
- ☐ 172.20.118.144
- ☐ 172.20.118.152
- ☐ 172.20.118.155
- ☐ 172.20.118.169
- ☐ 172.20.118.200

2 device(s) selected

Poller Details

Name *: myCustomPoller

Polling Interval: 5 Minutes

Templates *

Available Templates: CPU Utilization, Device Availability, EnergyWise Device, EnergyWise Port Po, Environmental Temp, Interface Availability, Interface Errors, Interface Utilization, Memory Utilization, PoE PORT Utilizatio

Selected Templates: CPU Utilization

Poller Preferences

☐ Poll all Instances

☐ Threshold Only

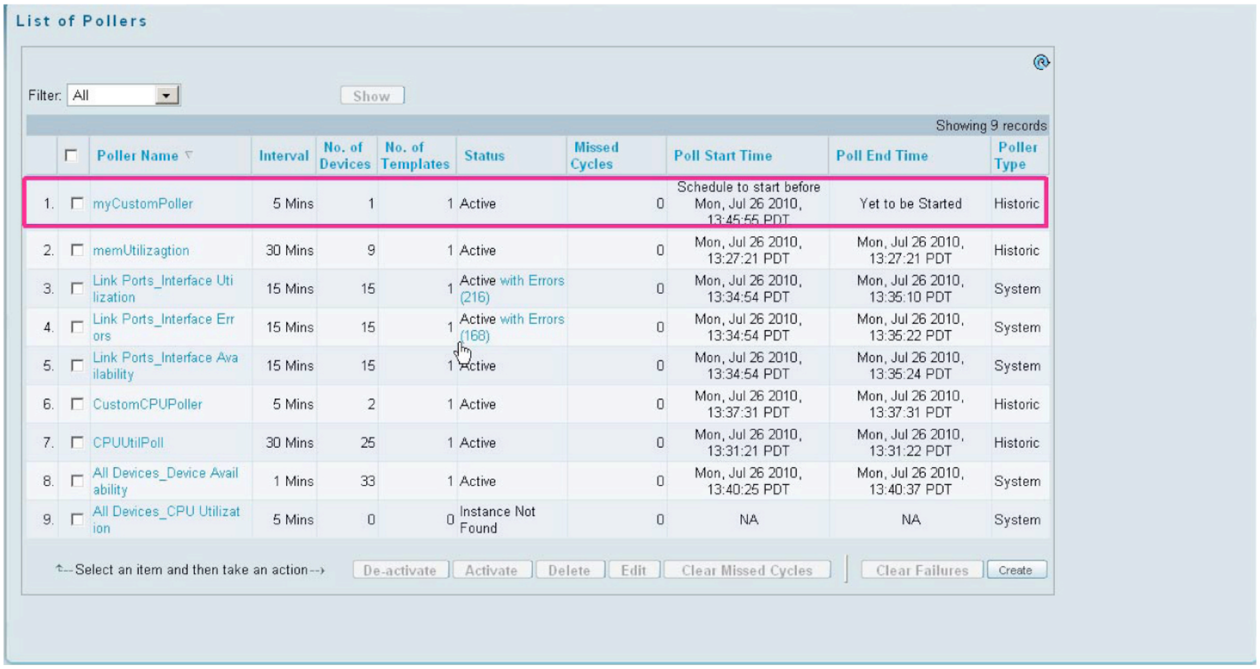
* - Required

- Step 1 of 3 -

Choose the instances from the next screen and click **Next**.

The poller, myCustomPoller, appears in the list of pollers in Figure 64.

Figure 64. Pollers



List of Pollers

Filter: All

Showing 9 records

	□	Poller Name	Interval	No. of Devices	No. of Templates	Status	Missed Cycles	Poll Start Time	Poll End Time	Poller Type
1.	□	myCustomPoller	5 Mins	1	1	Active	0	Schedule to start before Mon, Jul 26 2010, 13:45:55 PDT	Yet to be Started	Historic
2.	□	memUtilizagtion	30 Mins	9	1	Active	0	Mon, Jul 26 2010, 13:27:21 PDT	Mon, Jul 26 2010, 13:27:21 PDT	Historic
3.	□	Link Ports_Interface Utilization	15 Mins	15	1	Active with Errors (216)	0	Mon, Jul 26 2010, 13:34:54 PDT	Mon, Jul 26 2010, 13:35:10 PDT	System
4.	□	Link Ports_Interface Errors	15 Mins	15	1	Active with Errors (168)	0	Mon, Jul 26 2010, 13:34:54 PDT	Mon, Jul 26 2010, 13:35:22 PDT	System
5.	□	Link Ports_Interface Availability	15 Mins	15	1	Active	0	Mon, Jul 26 2010, 13:34:54 PDT	Mon, Jul 26 2010, 13:35:24 PDT	System
6.	□	CustomCPUPoller	5 Mins	2	1	Active	0	Mon, Jul 26 2010, 13:37:31 PDT	Mon, Jul 26 2010, 13:37:31 PDT	Historic
7.	□	CPUUtilPoll	30 Mins	25	1	Active	0	Mon, Jul 26 2010, 13:31:21 PDT	Mon, Jul 26 2010, 13:31:22 PDT	Historic
8.	□	All Devices_Device Availability	1 Mins	33	1	Active	0	Mon, Jul 26 2010, 13:40:25 PDT	Mon, Jul 26 2010, 13:40:37 PDT	System
9.	□	All Devices_CPU Utilization	5 Mins	0	0	Instance Not Found	0	NA	NA	System

IP SLA 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.

CiscoWorks LMS utilizes Cisco IOS IP SLA technology to monitor the end-to-end performance of multiprotocol networks. It measures performance from one end of the network to the other and allows a broader reach and more accurate representation of the end-user experience. Using IP SLA, IPM measures 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 http://www.cisco.com/go/ipsla.

Workflow for the IP SLA Monitoring

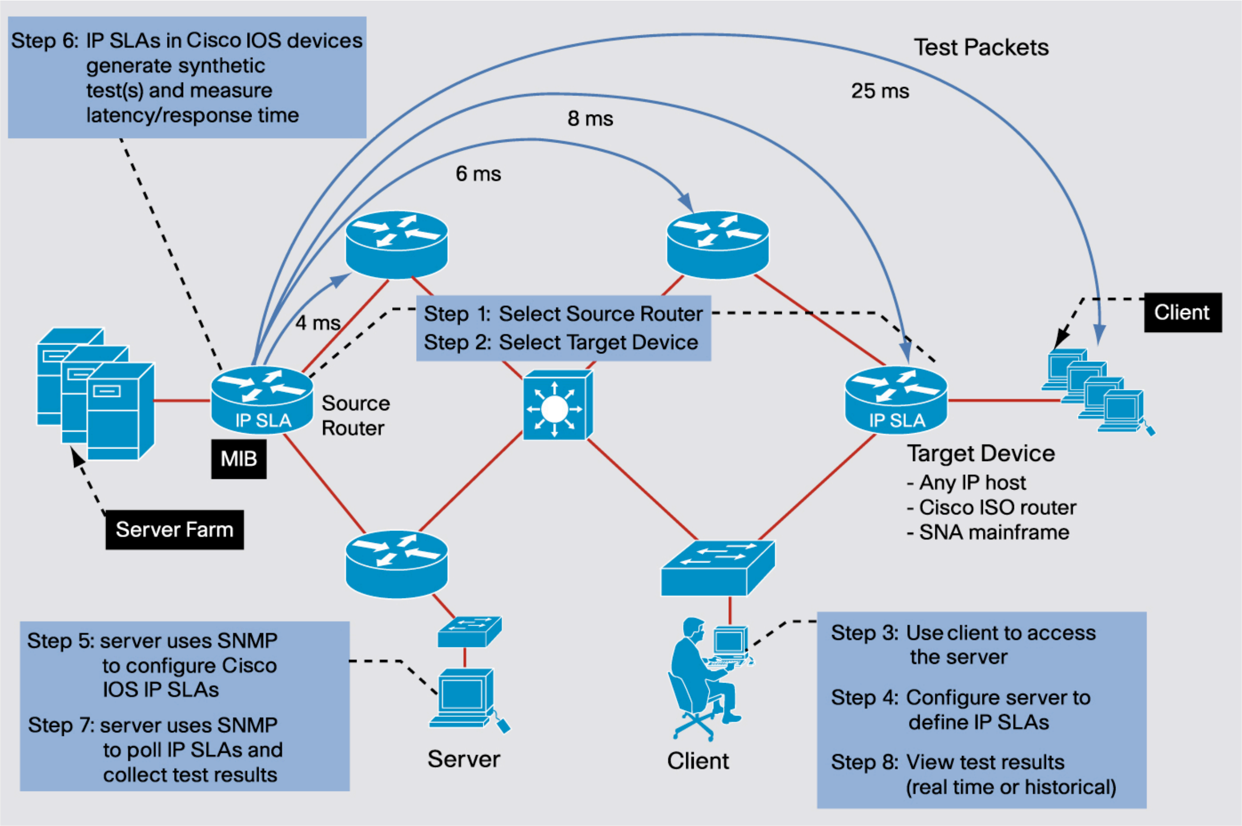
To use LMS for performance management, users need to define collectors to gather the performance data. A collector is made of four components,

- **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 IP SLA management is illustrated in Figure 65.

Figure 65. SLA Workflow


Step 6: IP SLAs in Cisco IOS devices generate synthetic test(s) and measure latency/response time
Test Packets
25 ms
8 ms
6 ms
4 ms
Step 1: Select Source Router
Step 2: Select Target Device
Client
IP SLA
Source Router
MIB
IP SLA
Target Device
- Any IP host
- Cisco ISO router
- SNA mainframe
Server Farm
Step 5: server uses SNMP to configure Cisco IOS IP SLAs
Step 7: server uses SNMP to poll IP SLAs and collect test results
Server
Client
Step 3: Use client to access the server
Step 4: Configure server to define IP SLAs
Step 8: View test results (real time or historical)

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 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.

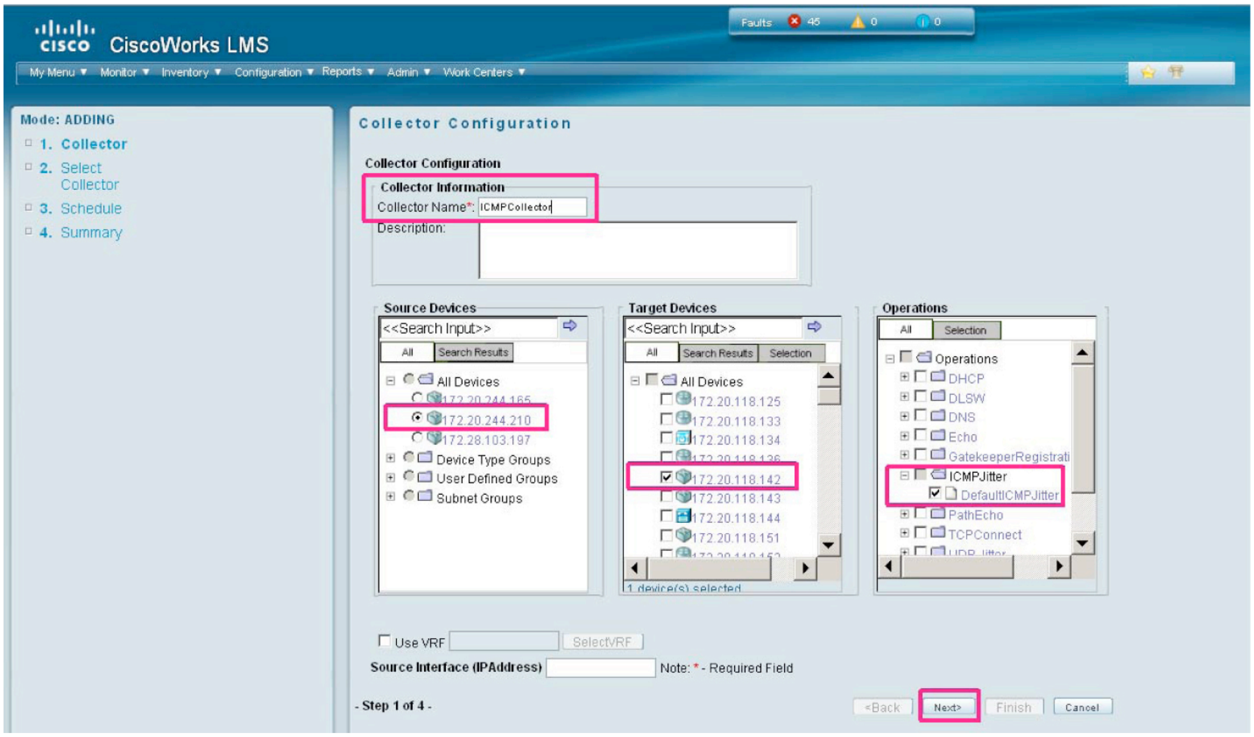
Define an Operation

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 Figure 66.

Figure 66. Create a Collector



Collector Configuration

Collector Information

Collector Name*: ICMPCollector

Description:

Source Devices: ● 172.20.244.210

Target Devices: ☑ 172.20.118.142

1 device(s) selected

Operations: ICMPJitter ☑ DefaultICMPJitter

Source Interface (IPAddress)

Note: * - Required Field

- Step 1 of 4 -

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 CiscoWorks LAN Management Solution 4.0 provides a single launch point for all the reports that can be generated and viewed in CiscoWorks LMS 4.0.

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, Power over 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 IP SLA reports.

- Cisco.com
- System

  These contain

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

- Audit

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

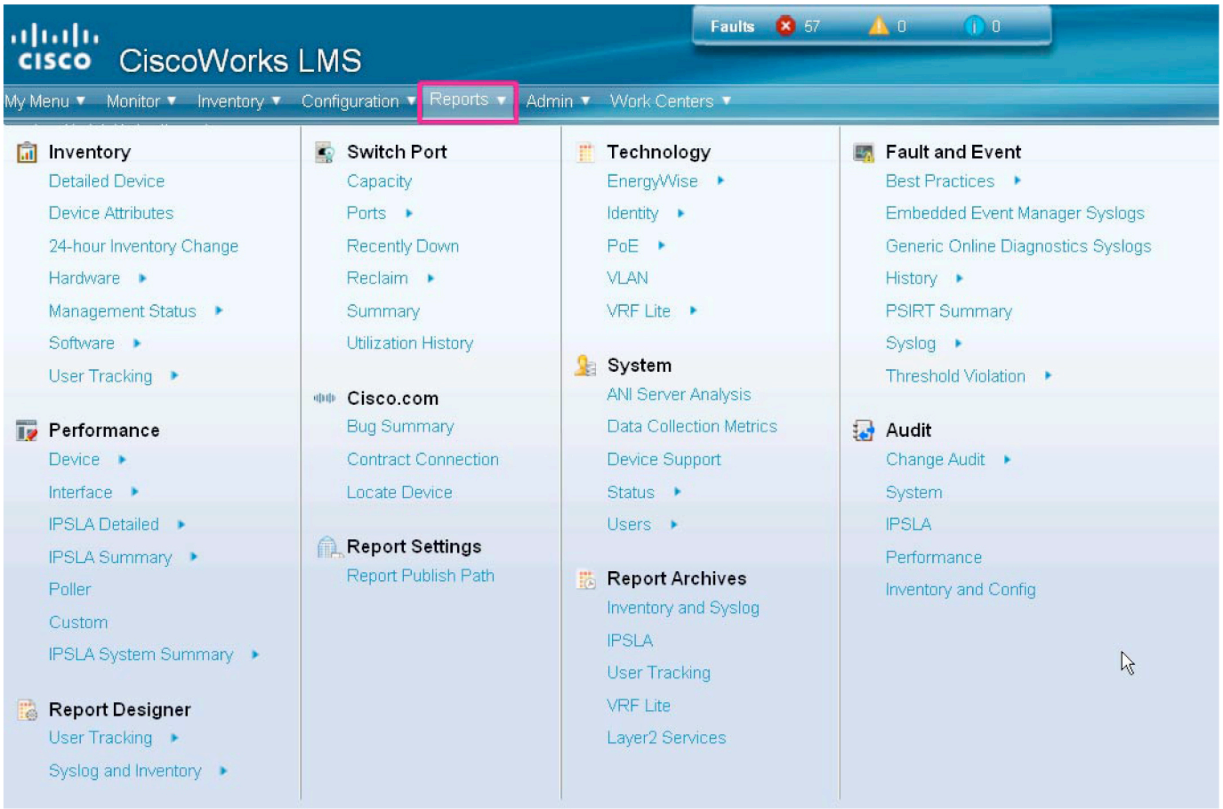
- Report Designer

  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. See Figure 67.

Figure 67. Archive Reports



Report Generation and Viewing Paradigm

Use case: We want to generate a detailed hardware report for a few devices. See Figures 68 and 69.

Figure 68. Select the Detailed Hardware Report

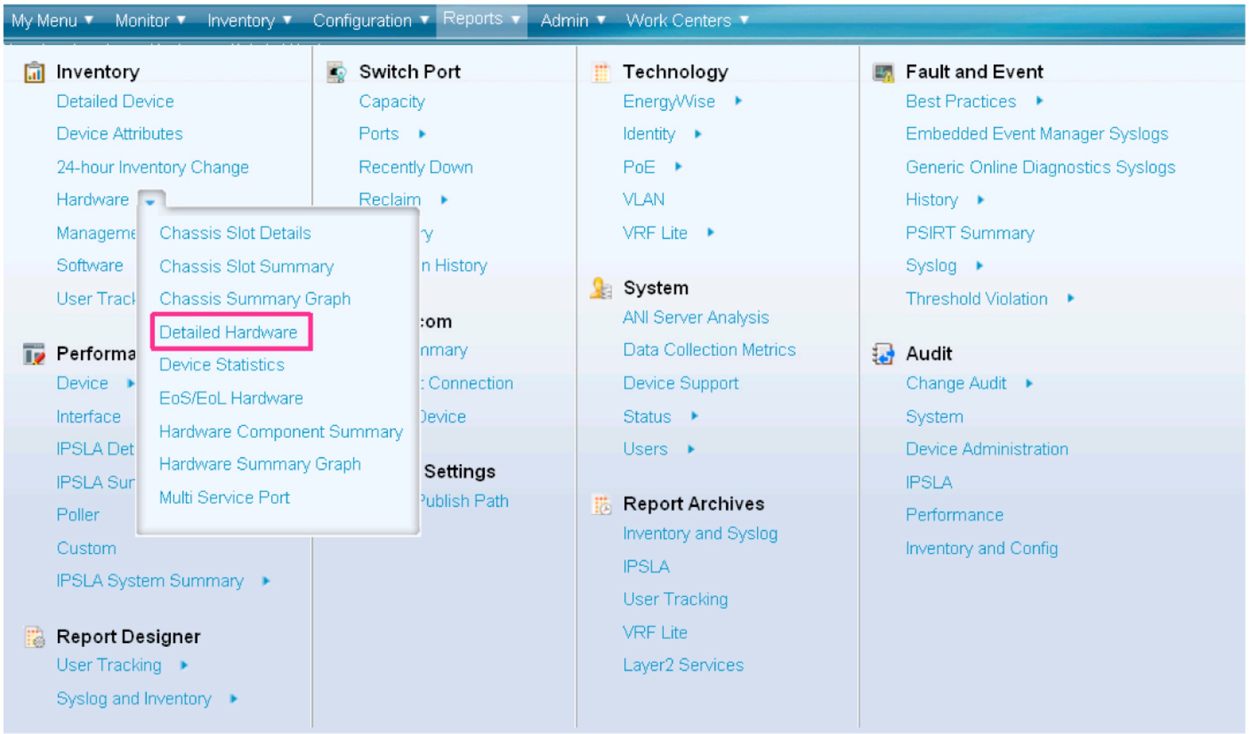
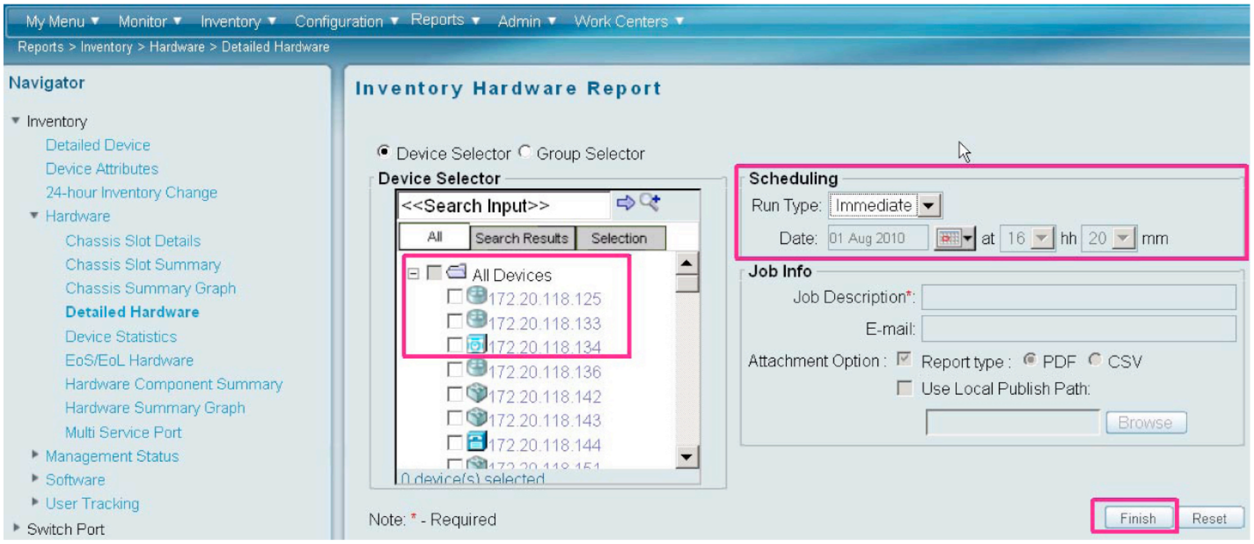


Figure 69. Select Devices and Schedule the Report



Inventory Hardware Report

● Device Selector ○ Group Selector

Device Selector

<<Search Input>>

□ All Devices
□ 172.20.118.125
□ 172.20.118.133
□ 172.20.118.134
□ 172.20.118.136
□ 172.20.118.142
□ 172.20.118.143
□ 172.20.118.144
□ 172.20.118.151

0 device(s) selected

Scheduling

Run Type: Immediate

Date: 01 Aug 2010 at 16 hh 20 mm

Job Info

Job Description*:

E-mail:

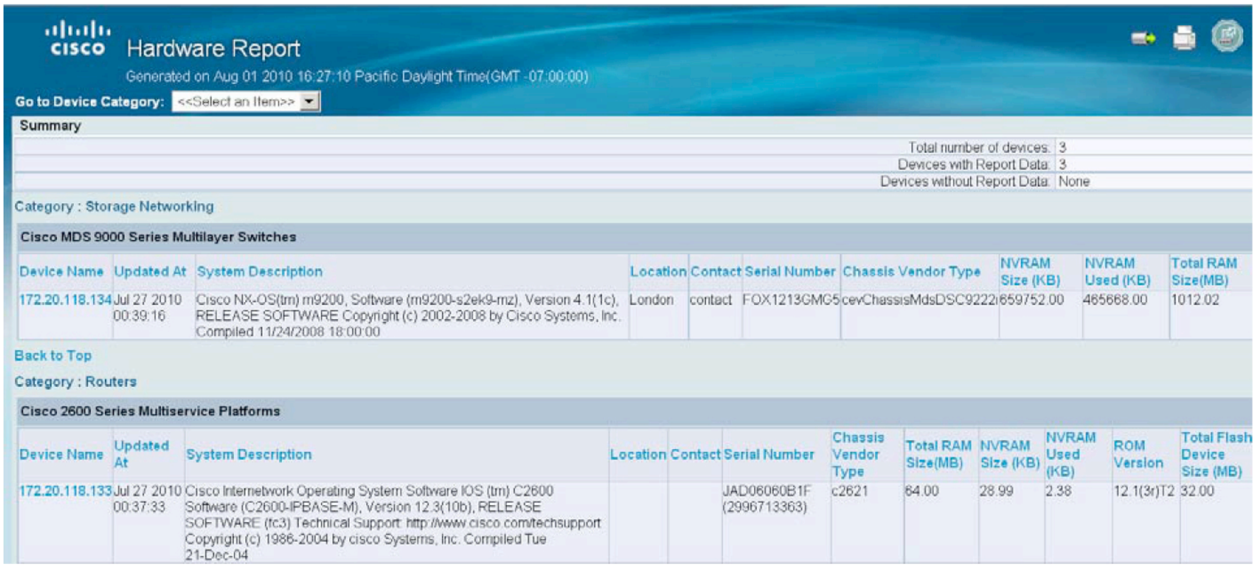
Attachment Option : ☑ Report type : ● PDF ○ CSV

□ Use Local Publish Path:

Note: * - Required

- 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 will be generated immediately and will look as in Figure 70.

Figure 70. Hardware Report



Hardware Report

Generated on Aug 01 2010 16:27:10 Pacific Daylight Time(GMT -07:00:00)

Summary

Total number of devices:	3
Devices with Report Data:	3
Devices without Report Data:	None

Category : Storage Networking

Cisco MDS 9000 Series Multilayer Switches

Device Name	Updated At	System Description	Location	Contact	Serial Number	Chassis Vendor Type	NVRAM Size (KB)	NVRAM Used (KB)	Total RAM Size(MB)
172.20.118.134	Jul 27 2010 00:39:16	Cisco NX-OS(tm) m9200, Software (m9200-s2ek9-mz), Version 4.1(1c), RELEASE SOFTWARE Copyright (c) 2002-2008 by Cisco Systems, Inc. Compiled 11/24/2008 18:00:00	London	contact	FOX1213GMG5	cevChassisMdsDSC9222i	659752.00	465668.00	1012.02

Category : Routers

Cisco 2600 Series Multiservice Platforms

Device Name	Updated At	System Description	Location	Contact	Serial Number	Chassis Vendor Type	Total RAM Size(MB)	NVRAM Size (KB)	NVRAM Used (KB)	ROM Version	Total Flash Device Size (MB)
172.20.118.133	Jul 27 2010 00:37:33	Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-IPBASE-M), Version 12.3(10b), RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2004 by cisco Systems, Inc. Compiled Tue 21-Dec-04			JAD06060B1F (2996713363)	c2621	64.00	28.99	2.38	12.1(3r)T2	32.00

Work Centers

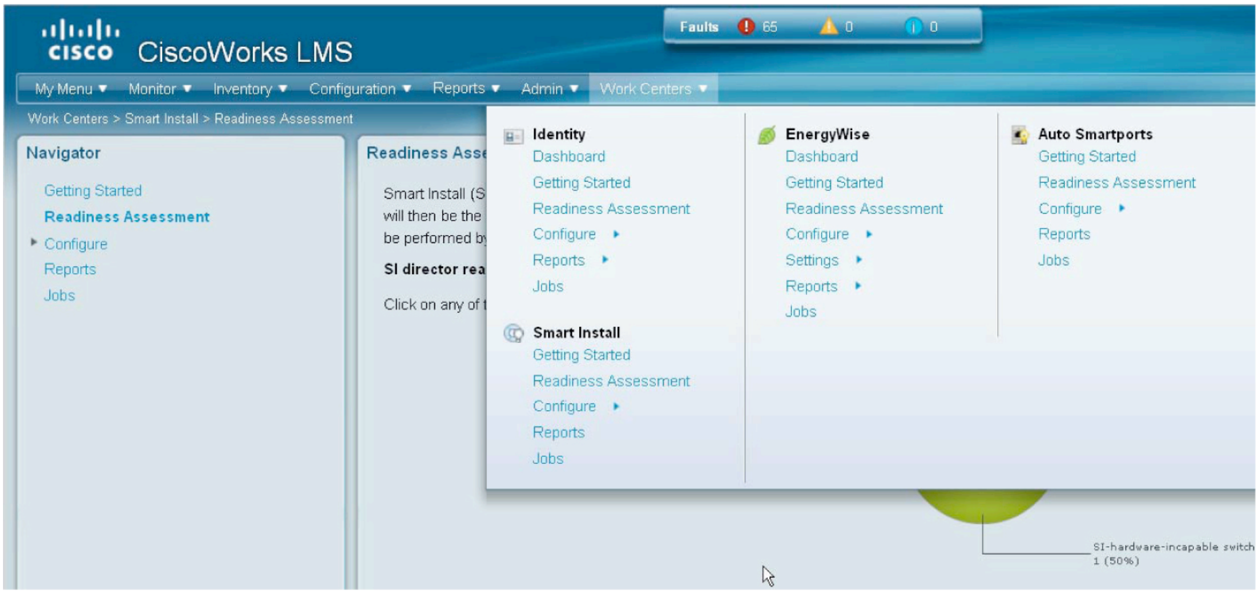
CiscoWorks LMS 4.0 provides complete lifecycle management of:

- Cisco solutions such as:
  - Identity
  - EnergyWise

- Network features such as:
  - Auto Smartports
  - Smart Install

LMS 4.0 provides a workflow-oriented approach for Day-1 to Day-n operations of Identity, EnergyWise, Auto Smartports, and Smart Install. This workflow includes readiness assessment, configuration, monitoring, reporting, and troubleshooting. See Figure 71.

Figure 71. Work Centers



A detailed description of each of these work centers will be discussed in a separate whitepaper named "Using Work Centers in LMS 4.0."

Server Administration

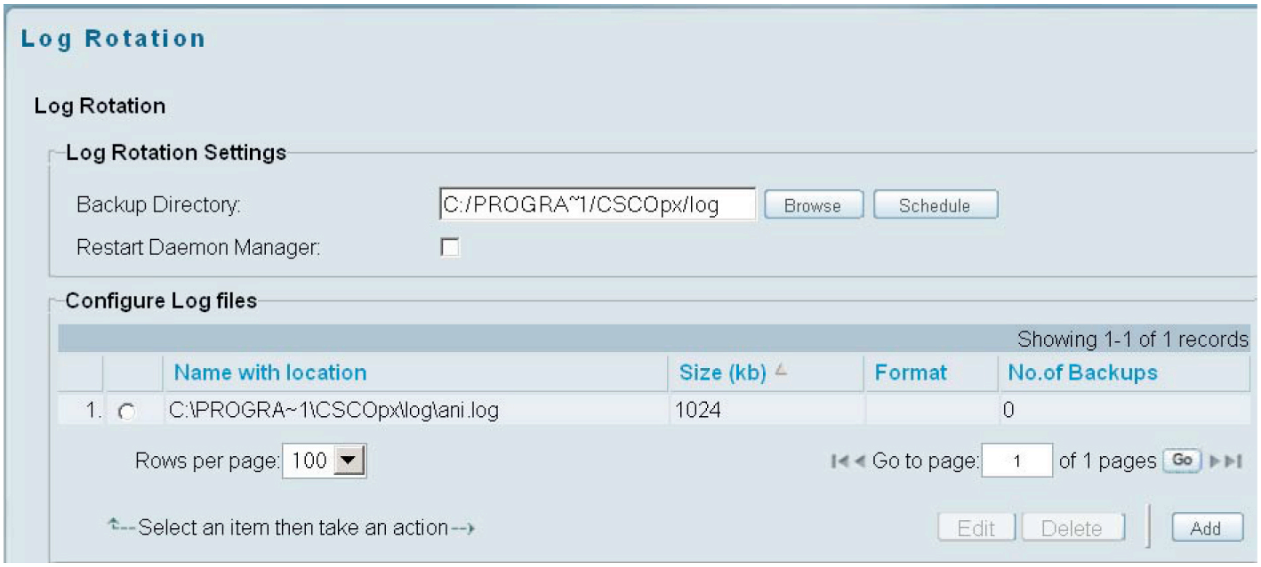
This chapter deals with server administration to optimally utilize the resources of the server while also maintaining a current status of the network topology.

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 72.

Figure 72. Log Rotation



Log Rotation

Log Rotation

Log Rotation Settings

Backup Directory: C:/PROGRA~1/CSCOpx/log

Restart Daemon Manager: □

Configure Log files

Showing 1-1 of 1 records

		Name with location	Size (kb)	Format	No.of Backups
1.	○	C:\PROGRA~1\CSCOpx\log\ani.log	1024		0

Rows per page: 100

Go to page: 1 of 1 pages

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

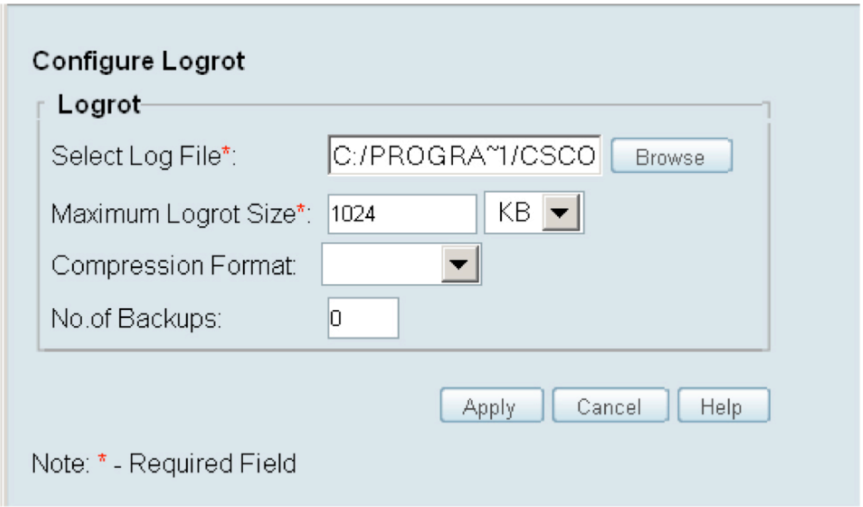
- NMSROOT\log on Windows
- /var/adm/CSCOpx/log on Solaris

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

Figure 73. Configure Logrot



Configure Logrot

Logrot

Select Log File*: C:/PROGRA~1/CSCO

Maximum Logrot Size*: 1024 KB

Compression Format:

No.of Backups: 0

Note: * - Required Field

As shown in Figure 73, you specify the log file name, maximum logrot size (the default is 1024 KB, the maximum size is 4096 MB), 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 back up 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:

- CiscoWorks user 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 and Solaris:

- On Windows, run:

  ```
  NMSROOT\bin\perl NMSROOT\bin\backup.pl <BackupDirectory> <[LogFile]>
  [Num_Generations]
  ```

- On Solaris, 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, 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

To restore the data on Solaris:

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 [-t temporary directory] [-gen generationNumber] [-d backup directory] [-h]
   Where:
   - [-t temporary 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*
   - [-gen generationNumber]: Optional. By default, it is the latest generation. If generations 1 through 5 exist, then 5 will be the latest.
   - [-d backup 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

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

   `where NMSROOT is the CiscoWorks installation 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.

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 in to 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 log in 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	Per VLAN Spanning Tree Protocol
RCP	Remote Copy Protocol

Acronym/Feature	Meaning
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 transparently navigate to multiple CiscoWorks servers without having to authenticate to each server.
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 log in 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 CiscoWorks 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
VTP	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.**

Printed in USA C07-618226-00 09/10