



Getting Started with CiscoWorks LAN Management Solution 4.0

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Getting Started with CiscoWorks LAN Management Solution
© 1998-2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface ix

- Audience ix
- Document Conventions x
- Product Documentation x
- Obtaining Documentation and Submitting a Service Request xii

Notices xiii

- OpenSSL/Open SSL Project iii-xiii
- License Issues iii-xiii

CHAPTER 1

Getting Started Overview 1-1

- Accessing CiscoWorks Server 1-1
 - Clearing Cache and Cookies 1-2
- Logging into CiscoWorks Server 1-3
- Getting Started Workflow in CiscoWorks LMS 1-3
- Supported Browser Versions 1-4
 - Displaying Popup Dialog Boxes 1-5
 - Disabling Address and Status Bars In Popup Dialog Boxes 1-5
 - Enabling Modal Dialog Boxes Support 1-6
 - Disabling Tabbed Browsing In Popup Windows 1-7
 - Enabling Reports Download In CSV and PDF Format 1-7
 - Enabling the Telnet protocol handler in IE 7 and IE 8 1-8
 - Launching CiscoWorks from Windows 2008 client 1-8

CHAPTER 2

Getting Started Workflow 2-1

- Configuring LMS Using the Getting Started Wizard 2-2
- Viewing LMS Dashboard 2-4
- Setting Getting Started as the Default Launch Page 2-4

CHAPTER 3

Understanding the CiscoWorks LMS Interface 3-1

- Understanding the Banner Interface Elements 3-1
- Navigating Menus 3-2
 - Understanding My Menu 3-2
 - My Dashboard 3-3

- Public Dashboard 3-3
- Default Dashboard 3-3
- Understanding Monitor Menu 3-3
- Understanding Inventory Menu 3-5
- Understanding Configuration Menu 3-7
- Understanding Reports Menu 3-10
- Understanding Admin Menu 3-12
- Understanding Work Centers Menu 3-15
- Adding and Configuring Portlets 3-16
 - Adding Portlets 3-16
 - Adding Frequently Used Links Portlet 3-17
 - Adding External Links Portlet 3-19
 - Adding Portlets From the Remote Server 3-19
 - Adding RSS Portlet 3-20
 - Adding IFrame Portlet 3-21
 - CiscoWorks Product Updates 3-23
 - Understanding Portlet Icons 3-23
 - Launching Portlets 3-24
 - Configuring Portlets 3-24
 - Changing the Title of a Portlet 3-25
- Changing the Portal Layout 3-25
- Adding and Configuring Dashboards 3-28
 - Add Dashboards 3-28
 - Set Dashboard Types 3-28
 - Hide Dashboards 3-30
 - Copy Dashboard Contents to a New Dashboard 3-30
 - Delete Dashboards 3-31
 - Set Default Dashboard 3-32
- Understanding the Search Bar 3-32
 - Understanding Global Search Results Page 3-33
- Understanding the Fault Bar 3-34
- Adding Links to Favorites 3-35
- Navigating Legacy Menu 3-35
- Using Online Help 3-35

CHAPTER 4

Dashboards in LMS 4-1

- Monitoring Dashboard 4-1
- Identity Dashboard 4-2

EnergyWise Dashboard	4-2
Inventory Dashboard	4-2
Configuration Dashboard	4-3
Device Status Dashboard	4-3
System Dashboard	4-4

CHAPTER 5

Configuring Multiserver Setup	5-1
Viewing the Current Server Settings	5-1
Converting the Server as Master or as Standalone	5-2
Converting the Server as Slave	5-2
Changing the Server Mode to DCR Standalone, Master and Slave	5-2
Changing the Mode to Standalone	5-2
Changing the Mode to Master	5-3
Changing the Mode to Slave	5-3
Changing the Server Mode to SSO Standalone, Master and Slave	5-4
Changing the SSO Mode to Standalone	5-5
Changing the SSO Mode to Master	5-5
Changing the SSO Mode to Slave	5-5
Adding Peer Server Certificates	5-6
Setting up System Identity Account	5-6

CHAPTER 6

Configuring E-mail, Cisco.com and Proxy Settings	6-1
E-mail Settings	6-1
Cisco.com Settings	6-2
Proxy Settings	6-2

CHAPTER 7

Updating Software and Device Packages and Migrating Data	7-1
Updating Software and Device Packages	7-1
Viewing Software and Device Packages Installed	7-1
Viewing Scheduled Job Details	7-3
Scheduling Software Updates and Device Package Downloads	7-5
Understanding the Procedure for Migrating Data	7-6

CHAPTER 8

Checking Protocol, Security, Backup and Authentication Settings	8-1
RCP and SCP Settings	8-1
Browser Server Security Settings	8-2
Backup Settings	8-2

Authentication Settings 8-3

CHAPTER 9

Managing User Roles and Users in LMS 9-1

- Managing Roles 9-1
 - Creating User Roles 9-1
 - Modifying User Roles 9-3
 - Copying User Roles 9-3
 - Deleting User Roles 9-4
 - Setting Default Roles 9-4
- Managing Users 9-4
 - Adding Users 9-4
 - Modifying Users 9-6
 - Deleting Users 9-7
 - Modifying User Profile 9-7

CHAPTER 10

Managing Devices and Credentials 10-1

- Allocating Devices 10-1
- Managing Devices using Functions 10-2
- Configuring Fallback to Secondary Credentials 10-3
- Configuring Credential Sets and Adding Devices 10-3
 - Configuring Credential Sets and Policies 10-4
 - Configuring Credential Sets 10-4
 - Configuring Credential Set Policies 10-5
- Adding Devices 10-6
 - Add Devices into DCR Through Discovery 10-6
 - Manually Add Devices to DCR 10-7
 - Import Devices into DCR 10-9

CHAPTER 11

Performing Advanced Configurations and Settings 11-1

- Configuring Auto Monitoring 11-1
- Configuring Identity 11-1
- Managing Faults 11-2
- Managing User Roles 11-2
- Managing Configurations 11-3
- Configuring EnergyWise 11-3
- Collection Settings 11-4
- Administering Groups 11-4

APPENDIX A

Troubleshooting Messages and Frequently Asked Questions in Getting Started A-A

Error Messages A-A

Frequently Asked Questions A-B

INDEX



Preface

CiscoWorks LAN Management Solution (LMS) provides you with powerful features that enable you to configure, monitor, troubleshoot, and administer networks.

CiscoWorks LMS 4.0 has a new menu layout that facilitates access to information and to the tools required to manage your network.

CiscoWorks LMS 4.0 groups tasks to the following core functions:

- Monitor
- Inventory
- Configuration
- Reports
- Admin
- Work Center

This guide provides information on the Getting Started feature in CiscoWorks LMS.

The Getting Started feature in CiscoWorks LMS 4.0 assists you in performing the configuration and setup tasks required to get your CiscoWorks LMS running, and to manage your Cisco networks.

This preface details the related documents that support the Getting Started feature, and demonstrates the styles and conventions used in this guide. This preface contains:

- [Audience](#)
- [Document Conventions](#)
- [Product Documentation](#)

Audience

This guide is for users who are skilled in network administration and management, and for network operators who use this guide to make configuration changes to devices using LMS. The network administrator or operator should be familiar with the following:

- Basic Network Administration and Management
- Basic Solaris System Administration
- Basic Windows System Administration
- Basic LMS Administration

Document Conventions

Table 1 describes the conventions followed in the user guide.

Table 1 **Conventions Used**

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font
Selecting a menu item in paragraphs	Option > Network Preferences
Selecting a menu item in tables	Option > Network Preferences



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Product Documentation



Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for updates.

Table 2 describes the product documentation that is available.

Table 2 **Product Documentation**

Document Title	Available Formats
<i>Getting Started with CiscoWorks LAN Management Solution 4.0 (this document)</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverworks_lan_management_solution/4.0/user/guide/getting_started/gug.html PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Context-sensitive online help</i>	Select an option from the navigation tree, then click Help.

Table 2 **Product Documentation**

Document Title	Available Formats
<i>Configuration Management with CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> • On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/user/guide/configuration_management/cmug.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Monitoring and Troubleshooting with CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> • On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/user/guide/monitoring_troubleshooting/mntug.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Inventory Management with CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> • On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/user/guide/inventory_mgmt/inventory.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Administration of CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> • On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/user/guide/admin/admin.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Technology Work Centers in CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> • On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/user/guide/work_centers/wc.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Reports Management with CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> • On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/user/guide/Reports/rptmgt_ug.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Installing and Migrating to CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> • On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/install/guide/install.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.

Table 2 **Product Documentation**

Document Title	Available Formats
<i>Navigation Guide for CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/navigation/guide/nav_guide.html PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Open Database Schema Support in CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/database_schema4.0/guide/dbviews.html PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Release Notes for CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/release/notes/lms40rel.html PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Supported Devices Table for CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/device_support/table/lms40sdt.html PDF version part of CiscoWorks LMS 4.0 Product DVD.
<i>Documentation Roadmap for CiscoWorks LAN Management Solution 4.0</i>	<ul style="list-style-type: none"> Printed document part of Software kit

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].



CHAPTER 1

Getting Started Overview

This chapter provides an overview of the Getting Started workflow in CiscoWorks LMS. The Getting Started workflow assists you in performing the tasks required to get your CiscoWorks LMS running, and to manage your networks.

When you login to CiscoWorks LMS Server for the first time, the Introduction page of the Getting Started workflow appears. The Introduction page lists the new features in CiscoWorks LMS 4.0.

This section explains the following:

- [Accessing CiscoWorks Server](#)
- [Logging into CiscoWorks Server](#)
- [Getting Started Workflow in CiscoWorks LMS](#)
- [Supported Browser Versions](#)

Accessing CiscoWorks Server

CiscoWorks LMS uses, by default, port number 1741 to access the CiscoWorks Server in normal (HTTP) mode and port number 443 to access the server in secure (HTTPS) mode.

To access the server from a client system, enter any one of these URLs in your web browser:

- If SSL is disabled and if you have installed the LMS applications on the default port, enter:

```
http://server_name:1741
```

- If SSL is enabled, and if you have installed the LMS applications on the default port, enter:

```
https://server_name:443
```

where *server_name* is the hostname of the server on which you have installed LMS applications.

The CiscoWorks Login page appears.

You can change the default web server port numbers (for HTTP and HTTPS modes) using the `changeport` utility. See *Administration of CiscoWorks LAN Management Solution 4.0* for more information.

On a Windows system, if you are using HPOV as your third party NMS application, you would require the IIS service to be enabled for HPOV to install and run. The IIS web server runs on SSL port 443, which is the default port for the LMS web server when installing CiscoWorks LMS.

To avoid a conflict, you should change the SSL port number of the LMS web server from 443 to another port that is available, and that has a number in the range 1026 to 65535.

**Note**

If you have accessed LMS earlier, we recommend you to clear the browser cache and delete cookies before logging into LMS 4.0 again. See [Clearing Cache and Cookies](#) for more information.

Clearing Cache and Cookies

The instructions for clearing the cache and cookies may be different for each browser and version. Here are the steps for deleting cache and cookies for the supported browsers and versions in LMS:

- [Internet Explorer 8](#)
- [Internet Explorer 7](#)
- [Mozilla FireFox 3.6.x](#)

Internet Explorer 8

To clear the cache and cookies:

-
- Step 1** Go to Tools menu.
 - Step 2** Select **Delete Browsing History**.
 - Step 3** Select the check box for **Temporary Internet Files and Cookies**.
 - Step 4** Click **Delete**.
 - Step 5** Once the files have been deleted, click **Okay**.
-

Internet Explorer 7

To clear the cache and cookies:

-
- Step 1** Go to Tools menu.
 - Step 2** Select **Delete Browsing History**.
 - Step 3** Click:
 - **Delete files** to delete Temporary Internet files
 - **Delete Cookies** to delete cookies.
 - Step 4** Click **Yes** in the confirmation window.
 - Step 5** Click **Close**.
-

Mozilla FireFox 3.6.x

To clear the cache and cookies:

-
- Step 1** Go to Tools menu.
- Step 2** Select **Clear Recent History**.
- Step 3** Select Everything from the Time Range to Clear drop-down list.
- Step 4** Select Details.
- Step 5** Select:
- **Cache** to clear the browser cache.
 - **Cookies** to delete the cookies.
- Step 6** Click **Clear Now**.
-

Logging into CiscoWorks Server

After you have accessed the CiscoWorks server, to login for the first time, do the following:

-
- Step 1** Enter the username in the Username field, and the password in the Password field of the Login page.
If you are an administrator, and logging in for the first time, use the admin password that you configured during installation.
- Step 2** Click **Login** or press **Enter**.
You are now logged into CiscoWorks server and the Getting Started Introduction page appears.
Contact the CiscoWorks Server Administrator if you are unable to login.
The new CiscoWorks LMS User Interface provides easy access to functions based menus, access to information portlets, searching objects, fault bar, icons for viewing favorites, viewing legacy navigation, adding portlets, changing dashboard layout, and more. See [Understanding the CiscoWorks LMS Interface](#) for more information.



Note Login sessions time out after two hours of inactivity. If the session is not used for two hours, you will be prompted to login again.

Getting Started Workflow in CiscoWorks LMS

The getting started workflow consists of a step-by-step wizard for configuring LMS after a fresh install. See [Getting Started Workflow](#) for more information.

Supported Browser Versions

You can invoke CiscoWorks home page using the following browsers:

- Microsoft Internet Explorer 7.0, 8.0.
- Mozilla Firefox 3.6.x

The above browsers are supported only on Windows client systems.

CiscoWorks applications use popup dialog boxes at many places. If you have a popup-blocker enabled in your browser, none of these popups will appear. Therefore, you should disable the popup-blocker if you have installed it.

[Table 1-1](#) lists the features and the issues that are available with the supported browsers:

Table 1-1 **Supported Browsers**

Browser Issues	Internet Explorer 7.0	Internet Explorer 8.0	Mozilla Firefox 3.6	See...
Popup windows are blocked by default	Yes	Yes	Yes	Displaying Popup Dialog Boxes
Popup windows appear with address bar	Yes	Yes	Yes	Disabling Address and Status Bars In Popup Dialog Boxes
Popup windows appear with status bar	Yes	Yes	No	Disabling Address and Status Bars In Popup Dialog Boxes
Modal dialog boxes supported by default	Yes	Yes	No	Enabling Modal Dialog Boxes Support
Links in a popup window open in a new tab, instead of a new window, by default (Tabbed browsing)	Not Applicable	Not Applicable	Yes	Disabling Tabbed Browsing In Popup Windows
Problems in exporting Reports to PDF and CSV Format on a Windows XP platform	Yes	Yes	Not Applicable	Enabling Reports Download In CSV and PDF Format
CiscoWorks does not launch from Windows 2008 client	Yes	Yes	No	Launching CiscoWorks from Windows 2008 client
Telnet protocol enabled	No	No	Yes	Enabling the Telnet protocol handler in IE 7 and IE 8

Displaying Popup Dialog Boxes

In Microsoft Internet Explorer 7.0 and 8.0, and Firefox 3.6 browsers, the popup dialog boxes are blocked and are not allowed to display:

To display the pop-up dialog boxes in Internet Explorer 7.0 and 8.0:

Step 1 Click **Tools > Pop-up Blocker**.

Step 2 Click:

- **Turn Off Pop-up Blocker** to turn off the pop-up blocker permanently and display the popup dialog boxes.

Or

- **Always Allow Pop-ups From This Site** to turn off the pop-up blocker only for CiscoWorks software.
-

To display the pop-up dialog boxes in Firefox 3.6:

Step 1 Click **Tools > Options**.

Step 2 Click the Content icon.

Step 3 Disable the Block pop-up windows option.

Step 4 Click **OK**.

Disabling Address and Status Bars In Popup Dialog Boxes

In Microsoft Internet Explorer 7.0 and 8.0, the popup dialog boxes and notification windows may appear with the address bar and the status bar enabled.

To disable the address bar in the popup dialog boxes in Microsoft Internet Explorer 7.0 and 8.0:

Step 1 Click **Tools > Internet Options**.

The Internet Options dialog box opens.

Step 2 Click the Security tab.

Step 3 Click **Custom level...** from the Security level for this zone panel.

The Security Settings dialog box opens.

Step 4 Select the Enable option for **Allow websites to open windows without address or status bars**.

Step 5 Click **OK**.

In Firefox 3.6, the popup dialog boxes and notification windows may appear with the address bar and the status bar enabled.

We recommend that you do not disable the address bar in the popup dialog boxes in Firefox 3.0.

If you disable the address bar in the popup dialog boxes in Firefox 3.6, close the browser windows and launch Firefox 3.6 or later, the address bar do not appear for the main browser windows.

You must disable the status bar in Firefox 3.6 to make the confirmation windows completely visible.

To disable the status bar in Firefox 3.6:

-
- Step 1** Click **Tools > Options**.
The Options dialog box opens.
 - Step 2** Click the Content icon.
 - Step 3** Click **Advanced...** to open the Advanced JavaScript Settings dialog box.
 - Step 4** Select **Hide the status bar**.
 - Step 5** Click **OK** to return to the Options dialog box.
 - Step 6** Click **OK**.
-

Enabling Modal Dialog Boxes Support

In Firefox 3.6 browsers, modal dialog boxes such as confirmation dialog boxes are not supported by default. They are supported in Internet Explorer browsers.

To enable the modal dialog boxes support in Firefox 3.6 browsers:

-
- Step 1** Click **Tools > Options**.
The Options dialog box opens.
 - Step 2** Click the Content icon.
 - Step 3** Click **Advanced...** to open the Advanced JavaScript Settings dialog box.
 - Step 4** Select **Raise or lower windows**.
 - Step 5** Click **OK** to return to the Options dialog box.
 - Step 6** Click **OK**.
-

Disabling Tabbed Browsing In Popup Windows

In Firefox 3.6 browser, you can open web pages in new tabs instead of opening them in new windows. This feature is enabled by default.

This behavior is the same when you open the pages from a popup window.

You can disable opening the pages in a new tab from a popup window in Firefox 3.6.

To do so:

-
- Step 1** Click **Tools > Options**.
The Options dialog box opens.
 - Step 2** Click the Tabs icon.
 - Step 3** Unselect the Open New windows for a new tab instead check box.
 - Step 4** Click OK.
-

Enabling Reports Download In CSV and PDF Format

In Microsoft Internet Explorer 7.0 and 8.0 browsers, sometimes problem occurs while exporting the reports in CiscoWorks applications to a PDF or CSV format. This problem occurs on a Windows XP client machine.

This may be caused by the default security settings in the browsers.

To enable exporting reports in CSV and PDF format in Internet Explorer browsers:

-
- Step 1** Click **Tools > Internet Options**.
The Internet Options dialog box opens.
 - Step 2** Click the Security tab.
 - Step 3** Click **Custom level...** from the Security level for this zone panel.
The Security Settings dialog box opens.
 - Step 4** Select the Enable option for the **File Download** and the **Automatic prompting for file downloads** fields.
 - Step 5** Click **OK**.
-

Enabling the Telnet protocol handler in IE 7 and IE 8

In Microsoft Internet Explorer 7.0 and 8.0 browsers, the Telnet protocol handler is disabled by default. To re-enable the Telnet protocol:

-
- Step 1** Click **Start > Run**.
The Run dialog box opens.
 - Step 2** In the Open box, enter: Regedit, then click OK.
The Registry Editor opens.
 - Step 3** Go to the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl.
 - Step 4** Under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl, create a new key named FEATURE_DISABLE_TELNET_PROTOCOL.
 - Step 5** Add a DWORD value named iexplore.exe and set the value to 0 (decimal).
 - Step 6** Close the Registry Editor.
 - Step 7** Restart Microsoft Internet Explorer 7. The Telnet protocol is enabled.
-

Launching CiscoWorks from Windows 2008 client

In Microsoft Internet Explorer 7.0 and 8.0 browsers, sometimes you cannot launch CiscoWorks from Windows 2008 client machine.

This is caused by the default security settings in the browsers.

To enable the META-REFRESH tag in the browser:

-
- Step 1** Click **Tools > Internet Options**.
The Internet Options dialog box opens.
 - Step 2** Click the Security tab.
 - Step 3** Select the Internet zone.
 - Step 4** Click **Custom level...**
The Security Settings dialog box opens.
 - Step 5** In the Miscellaneous options, select the Enable option for Allow Meta Refresh field.
 - Step 6** Click **OK**, and then **Apply** to update the settings.
 - Step 7** Close the IE 7 or IE 8 open windows.
 - Step 8** Launch a new IE 7 or IE 8 window and login into LMS.
-



CHAPTER 2

Getting Started Workflow

This chapter explains the Getting Started workflow in CiscoWorks LMS.

The LMS Getting Started workflow assistant helps you in performing the following tasks:

- [Understanding the Procedure for Migrating Data](#)
- [Configuring E-mail, Cisco.com and Proxy Settings](#)
- [Configuring Multiserver Setup](#)
- [Checking Protocol, Security, Backup and Authentication Settings](#)
- [Managing Devices and Credentials](#)
- [Managing User Roles and Users in LMS](#)
- [Updating Software and Device Packages](#)
- [Performing Advanced Configurations and Settings](#)

You can carry out these tasks in a sequential manner, using the Getting Started workflow. However, if you want to perform these tasks, independently, at different points in time, you can do so by selecting the required task from the Getting Started assistant pane on the right.

You can do the following from the Getting Started page:

- [Configuring LMS Using the Getting Started Wizard](#)
- [Viewing LMS Dashboard](#)
- [Setting Getting Started as the Default Launch Page](#)

Configuring LMS Using the Getting Started Wizard

The links at the bottom of the Getting Started page helps you to configure LMS using the wizard, or skip the wizard and launch the Device Status dashboard in LMS.

To configure LMS using the Getting Started wizard:

Step 1 Login to CiscoWorks LMS by entering the User name and Password.

The Introduction page of the Getting Started workflow appears, displaying:

- What's New in LMS 4.0, which shows the enhancements, new technologies, and new features supported in LMS 4.0:
 - Improved Usability
 - EnergyWise
 - Identity
 - Auto Smartports
 - Smart Install
 - Monitoring
 - Report Center
 - Enhanced Troubleshooting Workflows
 - Template Center
 - Local CiscoWorks Authorization Mode
- The option to set Getting Started as the default page for next login (See [Setting Getting Started as the Default Launch Page](#))
- The link to proceed with the step-by-step Getting Started wizard, beginning with Data Migration (See [Understanding the Procedure for Migrating Data](#))
- The link to skip the remaining workflow and proceed to Device Status dashboard (See [Device Status Dashboard](#))

Step 2 Proceed to **Data Migration** to view the data migration procedure.

The Data Migration page appears, displaying the steps for migrating data from an earlier version or the same version of LMS.

See [Understanding the Procedure for Migrating Data](#) for more information.

Step 3 Proceed to **General System Settings** to configure the following:

- E-mail Settings
- Cisco.com Credentials
- Proxy Settings

See [Configuring E-mail, Cisco.com and Proxy Settings](#) for more information.

Step 4 Proceed to **Multiserver Configuration** to view the current LMS server mode details.

You can change the DCR and Single sign-on (SSO) server modes from this page.

See [Configuring Multiserver Setup](#) for more information.

- Step 5** Proceed to **Other System Settings** to setup the LMS system.
- The System Settings page appears, where you can configure the following:
- RCP and SCP settings
 - Browser Server Security Mode setup
 - Backup settings
 - Authentication Mode settings
- See [Checking Protocol, Security, Backup and Authentication Settings](#) for more information.
- Step 6** Proceed to **Device Allocation Settings** for managing devices automatically and also managing devices using LMS functions.
- The Device Allocation Settings page appears, displaying the following for allocating and managing devices:
- Device allocation settings—You can automatically allocate all devices or allocate devices based on policies. If you disable auto allocate all devices, then you must configure policies to allocate devices based on the policies.
 - Functions that manage devices—You can select the LMS functions the will manage the devices.
- See [Managing Devices and Credentials](#) for more information.
- Step 7** Proceed to **Device Addition** and add devices to DCR, and to create credential sets and policies.
- You can:
- Create and manage credentials sets and assign them while adding devices.
 - Configure policies based on the credential sets.
 - Add devices to DCR using device discovery, add devices manually, or import devices using the bulk import option.
- See [Managing Devices and Credentials](#) for more information.
- Step 8** Proceed to **Manage Roles** to create and manage user roles in LMS.
- You can add, edit and delete roles for a user. You can assign LMS tasks for user roles.
- See [Managing Roles](#) for more information.
- Step 9** Proceed to **Manage Users** to manage users and their associated roles.
- The Manage Users page appears.
- You can add, edit and delete users and their associated roles. You can also set the authentication modes for users.
- See [Managing Users](#) for more information.
- Step 10** Proceed to **Software and Device Updates** to schedule and download software and device packages from Cisco.com.
- The Software and Device Package page appears, allowing you to do the following:
- View the details of the software and device packages that are currently installed.
 - Schedule jobs for downloading software updates and device packages.
 - View the details of download jobs for software updates and device packages.
- See [Updating Software and Device Packages and Migrating Data](#) for more information.
- Step 11** Proceed to **Advanced Configuration**.
- The Advanced Configurations page appears.

You can do the following configurations and settings from this page:

- Monitoring configurations—Select the Link Port groups or All Devices group and monitor the inter-link switches automatically.
- Configuration management—Deploy and manage configurations using Template Center.
- Identity configuration—Use the management functions, provided by LMS, that simplify and automate the Identity management lifecycle.
- EnergyWise configuration—Use the management functions, provided by LMS, that simplify and automate the energy management lifecycle of network infrastructure, and of devices attached to the network.
- Fault management—Manage faults by adjusting polling parameters.
- Collection settings—View and administer collection settings.
- User Role management—Manage Users and User Roles by assigning privileges to the users. User authorization is based on these privileges.
- Group administration—Create, manage, view, and delete device groups.

See [Performing Advanced Configurations and Settings](#) for more information.

Step 12 Click **Apply** to complete the Getting Started workflow in LMS.

The Device Status dashboard page appears, displaying the portlets.

Viewing LMS Dashboard

Dashboards provide you with a quick snapshot of specific functions in LMS. See [Dashboards in LMS](#) for more information.

Setting Getting Started as the Default Launch Page

You can set the Getting Started page as the default page to appear whenever you login to LMS by unselecting the check box **Do not show Getting Started wizard at next login** in the Getting Started Introduction page. This option is selected by default.



CHAPTER 3

Understanding the CiscoWorks LMS Interface

This chapter provides a brief description of the elements in the CiscoWorks LMS user interface. It explains:

- [Understanding the Banner Interface Elements](#)
- [Navigating Menus](#)
- [Adding and Configuring Portlets](#)
- [Changing the Portal Layout](#)
- [Adding and Configuring Dashboards](#)
- [Understanding the Search Bar](#)
- [Understanding the Fault Bar](#)
- [Adding Links to Favorites](#)
- [Navigating Legacy Menu](#)
- [Using Online Help](#)





Understanding the Banner Interface Elements

The [Table 3-1](#) describes the elements and icons in the portal banner interface.

Table 3-1 Portal Interface Element Description

Element/Icon	Function
Sitemap	Contains an organized listing of links to all the pages in LMS.
User	Shows the name of the user who is logged into the application. For example, Admin.
Logout	Enables you to exit from the application.
About	Enables you to see the license details of the application. You can click the links displayed in the page to see the purchase licence information.
Help	Launches the context-sensitive online help. The window also contains buttons that take you to the overall help contents, index, and search tools.
Search Bar	Enables you to search for devices, end hosts, tasks, jobs and help topics. See Understanding the Search Bar for more information.

Table 3-1 Portal Interface Element Description

Element/Icon	Function
 (Favorites)	Enables you to add you frequently used links here. See Adding Links to Favorites for more information.
 (Legacy)	Enables you to access LMS tasks and features using the legacy LMS 3.x navigation path. See Navigating Legacy Menu for more information.
 (Add Portlets)	Enables you to add portlets. For more information on adding a portlet, see Adding Portlets .
 (Change Layout)	Enables you to arrange the portlets in different groups. Changing the Portal Layout for more information.
Refresh	Reloads the page and displays the latest data of the portlets.

Navigating Menus

This section describes the menus available in LMS. It also explains the sub-menu items in each function menu.

The menus are explained as:

- [Understanding My Menu](#)
- [Understanding Monitor Menu](#)
- [Understanding Inventory Menu](#)
- [Understanding Configuration Menu](#)
- [Understanding Reports Menu](#)
- [Understanding Admin Menu](#)
- [Understanding Work Centers Menu](#)

Understanding My Menu

My Menu helps you to consolidate information that is specific to a particular function as dashboards. It also enables you to group data from different functions into a single page. You can add, view and manage dashboards using:

- [My Dashboard](#)
- [Public Dashboard](#)
- [Default Dashboard](#)

My Dashboard

My Dashboard lists the dashboards created by you. These user-defined dashboards can be accessed only by the user who created them and not by others.

Public Dashboard

You can add or modify portlets or dashboards from the public dashboard list. Public dashboards can be accessed by all users.

Default Dashboard

The Default Dashboard displays links to the following system-defined dashboards in LMS:

- Configuration (See [Configuration Dashboard](#))
- Device Status (See [Device Status Dashboard](#))
- Inventory (See [Inventory Dashboard](#))
- Monitoring (See [Monitoring Dashboard](#))
- System (See [System Dashboard](#))
- EnergyWise (See [EnergyWise Dashboard](#))
- Identity (See [Identity Dashboard](#))

See [Dashboards in LMS](#) for more information.

Understanding Monitor Menu

You can use the Monitor menu for monitoring and troubleshooting devices in LMS. The menu also offers performance and fault management tasks and diagnostic tools.

[Table 3-2](#) describes the sub-menu items of the Monitor menu.

Table 3-2 Sub-menu items of the Monitor menu

Sub-Menu	Description
Dashboards	Links to the following dashboards in LMS: <ul style="list-style-type: none"> • Monitoring • Identity • EnergyWise
Diagnostic Tools	Links to the following diagnostic tools in LMS: <ul style="list-style-type: none"> • Embedded Event Manager • Generic Online Diagnostics

Table 3-2 Sub-menu items of the Monitor menu

Sub-Menu	Description
Threshold Settings	Links to the following threshold management options: <ul style="list-style-type: none"> • Fault • Apply Changes • Performance • TrendWatch
Monitoring Tools	Links to the following monitoring tools in LMS: <ul style="list-style-type: none"> • Fault Monitor • Event Monitor • Mini-RMON • Topology Services
Fault Settings	Links to the following fault management tasks in LMS: <ul style="list-style-type: none"> • Setup <ul style="list-style-type: none"> – Polling Parameters – Priority Settings – Apply Changes – Fault Device Details • SNMP Traps <ul style="list-style-type: none"> – Forwarding – Notification – Receiving • Syslog <ul style="list-style-type: none"> – Configure Syslog on Device – Message Filters – Automated Actions

Table 3-2 Sub-menu items of the Monitor menu

Sub-Menu	Description
Troubleshooting Tools	<p>Links to the following Troubleshooting tools in LMS:</p> <ul style="list-style-type: none"> • NetShow <ul style="list-style-type: none"> – Assigning Command Sets – Command Sets – NetShow Jobs – Output Archive • Troubleshooting Workflows • VRF Lite <ul style="list-style-type: none"> – Ping and Traceroute – Show Commands
Performance Settings	<p>Links to the following performance management tools in LMS:</p> <ul style="list-style-type: none"> • Setup <ul style="list-style-type: none"> – Automonitor – Pollers – Templates • Receiver Groups • IPSLA <ul style="list-style-type: none"> – Collectors – Operations – Outage Settings – Devices

For more information, see *Monitoring and Troubleshooting with CiscoWorks LAN Management Solution 4.0*.

Understanding Inventory Menu

You can use the Inventory menu for discovering network devices, managing device credentials, generating inventory and device reports, and managing inventory dashboards.

[Table 3-3](#) describes the sub-menu items of the Inventory menu.

Table 3-3 Sub-menu items of the Inventory menu

Sub-Menu	Description
Dashboard	Links to the following dashboards in LMS: <ul style="list-style-type: none"> • Inventory • Device Status
User Tracking Settings	Links to view user tracking details in LMS: <ul style="list-style-type: none"> • Acquisition Actions • Acquisition Summary
Device Administration	Links to administer and allocate devices in LMS: <ul style="list-style-type: none"> • Add / Import / Manage Devices • Manage Device State • Discovery <ul style="list-style-type: none"> – Launch / Summary – Schedule – Settings • Device Aliases • Device Allocation Policy • Add as Managed Devices • IPSLA Devices • Auto Update Server Management
Tools	Links to the following tools in LMS: <ul style="list-style-type: none"> • CiscoView • Device Center • Mini-RMON • Smartcase
Group Management	Lists the following group management links in LMS: <ul style="list-style-type: none"> • Device • Fault • IPSLA Collector • Port and Module
Job Browsers	Links to access and manage the following job browsers: <ul style="list-style-type: none"> • Device Credentials Verification • Inventory Collection

For more information, see *Inventory Management with CiscoWorks LMS 4.0*.

Understanding Configuration Menu

You can use the Configuration menu for deploying configurations on devices, updating software images, archiving and comparing configuration files, configuring Cisco technologies and VLANs, and converting standalone switches to a virtual switching system. Configuration menu also offers compliance tasks using which you can generate configuration compliance reports.

Table 3-4 describes the sub-menu items of the Configuration menu.

Table 3-4 Sub-menu items of the Configuration menu

Sub-Menu	Description
Dashboard	Link to access the Configuration Dashboard
Compliance	<p>Links to check for configuration compliance, deploy configurations, generate out-of-sync summary report:</p> <ul style="list-style-type: none"> • Compliance Templates <ul style="list-style-type: none"> – Templates – Compliance Check – Direct Deploy – Jobs • Out-of-Sync Summary
Job Browsers	<p>Links to access and manage the following job browsers in LMS:</p> <ul style="list-style-type: none"> • Compliance • Configuration Archive • Template Center • NetConfig • Software Image Management • Config Editor • VRF Lite • Job Approval

Table 3-4 Sub-menu items of the Configuration menu

Sub-Menu	Description
Tools	<p>Links to the following configuration tools and options:</p> <ul style="list-style-type: none"> • Template Center <ul style="list-style-type: none"> - Deploy - Manage - Import - Assign Template to User - Jobs • NetConfig <ul style="list-style-type: none"> - Deploy - Assigning Tasks - User Defined Tasks • Config Editor <ul style="list-style-type: none"> - Config Editor - Private Configs - Public Configs - Edit Mode Preference • Software Image Management

Table 3-4 Sub-menu items of the Configuration menu

Sub-Menu	Description
Workflows	Links to access the following workflows in LMS: <ul style="list-style-type: none"> • VLAN <ul style="list-style-type: none"> - Configure VLAN - Delete VLAN - Create Private VLAN - Delete Private VLAN - Configure Port Assignment - Configure Promiscuous Ports - Create Trunk - Modify Trunk Attributes • VRF Lite <ul style="list-style-type: none"> - Create VRF - Edit VRF - Extend VRF - Delete VRF - Edge VLAN Configuration • Virtual Switching System <ul style="list-style-type: none"> - VSS Conversion - VSS Reverse Conversion
Configuration Archive	Links to manage configuration archives: <ul style="list-style-type: none"> • Summary • Views <ul style="list-style-type: none"> - Custom Queries - Search Archive - Version Summary - Version Tree • Synchronization • Compare Configs • Label Configs • Protocol Usage Summary
Topology	Link to launch Topology Services

For more information, see *Configuration Management with CiscoWorks LAN Management Solution 4.0*.

Understanding Reports Menu

You can use the Reports menu to view and generate reports such as device reports, fault and event reports, audit reports, inventory reports, performance reports, Cisco.com reports, system reports in LMS.

Table 3-5 describes the sub-menu items of the Reports menu.

Table 3-5 Sub-menu items of the Reports menu

Sub-Menu	Description
Inventory	Links to generate and view the following inventory reports: <ul style="list-style-type: none"> • Detailed Device • Device Attributes • 24-hour Inventory Change • Hardware • Management Status • Software • User Tracking
Performance	Links to generate and view the following performance reports: <ul style="list-style-type: none"> • Device • Interface • IPSLA Detailed • IPSLA Summary • Poller • Custom • IPSLA System Summary
Switch Port	Links to generate and view the following Switch port reports: <ul style="list-style-type: none"> • Capacity • Ports • Recently Down • Reclaim • Summary • Utilization History
Cisco.com	Links to generate and view the following Cisco.com reports: <ul style="list-style-type: none"> • Bug Summary • Contract Connection • Locate Device
Report Settings	Link to configure the report publish path.

Table 3-5 *Sub-menu items of the Reports menu*

Sub-Menu	Description
Technology	Links to generate and view the following Technology reports: <ul style="list-style-type: none"> • EnergyWise • Identity • PoE • VLAN • VRF Lite
System	Links to generate and view the following System reports: <ul style="list-style-type: none"> • ANI Server Analysis • Data Collection Metrics • Device Support • Status • Users
Report Archives	Links to view the following archived reports: <ul style="list-style-type: none"> • Inventory and Syslog • IPSLA • User Tracking • VRF Lite • Layer2 Services
Faults and Events	Links to generate the following reports for faults and events: <ul style="list-style-type: none"> • Best Practices • Embedded Event Manager Syslogs • Generic Online Diagnostics Syslogs • History • PSIRT Summary • Syslog • Threshold Violation

Table 3-5 Sub-menu items of the Reports menu

Sub-Menu	Description
Audit	Link to generate the following audit reports: <ul style="list-style-type: none"> • Change Audit • System • Device Administration • IPSLA • Performance • Inventory and Config
Report Designer	Links to generate the following custom reports: <ul style="list-style-type: none"> • User Tracking <ul style="list-style-type: none"> – Custom Reports – Custom Layouts • Syslog and Inventory <ul style="list-style-type: none"> – Custom Report Template

For more information, see *Reports Management with CiscoWorks LAN Management Solution 4.0*.

Understanding Admin Menu

You can use the Admin menu for performing all the network and system administration activities such as Device Credential Repository settings, Collection settings, tools settings, purge settings, report settings, group management, server administration, and software center.

[Table 3-6](#) describes the sub-menu items of the Admin menu.

Table 3-6 Sub-menu items of the Admin menu

Sub-Menu	Description
Getting Started	Link to launch the Getting Started workflow in LMS.
Dashboard	Links to launch the following admin dashboards: <ul style="list-style-type: none"> • System • Device Status
Trust Management	Links to configure the following server setups: <ul style="list-style-type: none"> • Local Server • Multi Server
Jobs	Links to access and manage Jobs: <ul style="list-style-type: none"> • Browser • Approval

Table 3-6 Sub-menu items of the Admin menu

Sub-Menu	Description
Collection Settings	Links to the following data collection settings: <ul style="list-style-type: none"> • Config • Data Collection • Fault • Inventory • Performance • Syslog • User Tracking • VRF Lite
Network	Links to perform the following network admin settings: <ul style="list-style-type: none"> • Change Audit Settings • Discovery Settings • PSIRT, EOS and EOL Settings • Configuration Job Settings • Device Credential Settings • Display Settings • Monitor / Troubleshoot • Notification and Action Settings • Purge Settings • Resource Browser • Software Image Management • Best Practices Deviation Settings

Table 3-6 Sub-menu items of the Admin menu

Sub-Menu	Description
System	Links to perform the following system settings: <ul style="list-style-type: none"> • Authentication Mode Setup • Backup • Cisco.com Settings • Debug Settings • Group Management • License Management • Log Rotation • Server Monitoring • Device Management Functions • SMTP Default Server • Software Center • System Preferences • User Management

For more information, see *Administration of CiscoWorks LAN Management Solution 4.0*.

Understanding Work Centers Menu

You can use Work Centers for configuring and managing Cisco technologies such as Identity, EnergyWise, Smart Install, and Auto Smartports on devices, using LMS.

[Table 3-7](#) describes the sub-menu items of the Work Centers menu.

Table 3-7 Sub-menu items of the Work Centers menu

Sub-Menu	Description
Identity	Links to view, configure and manage Identity on devices: <ul style="list-style-type: none"> • Dashboard • Getting Started • Readiness Assessment • Configure • Reports • Jobs
Auto Smartports	Links to view, configure and manage Auto Smartports on devices: <ul style="list-style-type: none"> • Getting Started • Readiness Assessment • Configure • Reports • Jobs
EnergyWise	Links to view, configure and manage EnergyWise solution on capable devices: <ul style="list-style-type: none"> • Dashboard • Getting Started • Readiness Assessment • Configure • Settings • Reports • Jobs
Smart Install	Links to view, configure and manage Smart Install solution on capable devices: <ul style="list-style-type: none"> • Getting Started • Readiness Assessment • Configure • Reports • Jobs

For more information, see *Technology Work Centers in CiscoWorks LAN Management Solution 4.0*.

Adding and Configuring Portlets

Portlets are the basic units of CiscoWorks LMS. They are features that can be plugged into, displayed in, and managed using the portal.

You can add portlets to any dashboard in CiscoWorks LMS.

This section explains:

- [Adding Portlets](#)
- [Understanding Portlet Icons](#)
- [Launching Portlets](#)
- [Configuring Portlets](#)
- [Changing the Title of a Portlet](#)

Adding Portlets

You can add a portlet to any dashboard in LMS. Portlets in LMS are grouped into two categories, CiscoWorks and Miscellaneous portlets.

- CiscoWorks portlets are function-based dashboard portlets that show information specific to network performance, monitoring, reporting, messages, device status, faults, alerts, inventory, and syslogs.
- Other CiscoWorks portlets are portlets used for adding external links, frequently used links, and remote server portlets. See [Adding Frequently Used Links Portlet](#), [Adding External Links Portlet](#), and [Adding Portlets From the Remote Server](#) for more information.
- Miscellaneous portlets are portlets used for viewing information that are not specific to LMS data. See [Adding RSS Portlet](#) and [Adding IFrame Portlet](#) for more information.

You can view the latest updates on CiscoWorks products using [CiscoWorks Product Updates](#) portlet.

To add a portlet:

Step 1 Click the Add Portlet icon at the top right corner of the CiscoWorks LMS page.

The Add portlet pop-up window appears.

- To expand the sections displayed, select the expand icon next to the section title.
- To collapse the sections displayed, select the collapse icon next to the section title.

Each section in this window contains a list of portlets.

Step 2 Click **Add** next to the name of a portlet.

The portlet is added to the selected Dashboard.

Step 3 Repeat this step as many times as necessary.

- If the portlet is multi-instance (allows you to add the same portlets more than once) the portlet name will continue to appear in the list. The multi-instance portlets are displayed with a green box against the respective portlet

For example, the RSS or IFrame portlets are multi-instance portlets. You can add these portlets as many times to any view.

- If the portlet is single-instance, a purple box is displayed against the name of the portlet. You can add this portlet only once to the View.
For example, if you want to view the Change Audit portlet, it displays only the audit details. Hence it is a single-instance portlet.
- If the portlet is already displayed in the particular view, the portlet name will be disabled.

You can also arrange the portlets in CiscoWorks LMS using the Change Layout option.

For more information on changing the layout, see [Changing the Portal Layout](#).

Step 4 Click **Close** to close the popup window

Adding Frequently Used Links Portlet

The Frequently Used Links portlet allows you to add the most commonly used links.

You can also add, modify, and remove the frequently accessed links. For details, see [Adding a New Link to the Frequently Used Links Portlet](#).

To add the Frequently Used Links portlet:

-
- Step 1** Click the Add Portlet icon at the top right corner of the CiscoWorks LMS page.
A popup window appears. Each section in this window contains a list of portlets.
You can expand and collapse the sections by clicking the arrows next to the section titles.
- Step 2** Click **CiscoWorks** and select **Others**.
A list of portlet names appears.
- Step 3** Click **Add** next to the Frequently Used Links portlet.
The Frequently Used Links portlet is displayed in the dashboard.
- Step 4** Click **Close** to close the popup window.
- Step 5** Move the mouse over the Frequently Used Links portlet to view the icons.
- Step 6** Click the Configuration icon.

The default link names in the Frequently Used Links portlet are displayed. These are:

- Local User Setup
- Add Device
- Log File Status
- Process Status

To add a new link to the Frequently Used portlet, see [Adding a New Link to the Frequently Used Links Portlet](#).



Note

Select the check box against the names to view the default links in the Frequently Used Links portlet.

Adding a New Link to the Frequently Used Links Portlet.

To add a new link:

Step 1 Click the configuration icon in the Frequently Used Links portlet.

The list of default link names is displayed in the portlet.

Step 2 Enter the new name in the Display Name field.

Step 3 Enter the URL in the URL field.

For example,

```
http://servername:port/rme/workcenter/identity/configRadius.jsp?navid=Identity_Configure_Radius
```

You can also use the relative path of the URL by removing `http://servername:port` from the URL

For example, `/rme/workcenter/identity/configRadius.jsp?navid=Identity_Configure_Radius`.

You must also add the `navid` along with the URL. In the above instance, the `navid` is `Identity_Configure_Radius`.

Step 4 Click **Add** to add the new link name.

The newly added link is added to the configuration screen and appears in bold.

Step 5 Click **Save** to save the new link and the name changes from bold to plain.

Or

Click **Reset** to clear all the newly added link names.



Note The link name changes from bold to plain only after it is saved.

Step 6 Select the check box against the newly added link name.

Click **Save** to save all the changes.

Editing and Deleting Link Names

You can edit and delete link names:

- Click the Edit button corresponding to the link to modify the link name.
- Click the Delete button corresponding to the link name to remove the link.

To re-arrange the links, click on the link name, drag it to the position of your choice, and drop it.

Adding External Links Portlet

You can view all information related to Cisco products and services, network solutions, integration solutions, documentation, network management, and custom tools using the External Links portlet.

Table 3-8 lists the External Links portlet details.

Table 3-8 External Links Portlet

Launch Points	Description
Cisco.com Resources	Click this link and expand to view the following technical support details. <ul style="list-style-type: none"> • Contact TAC • Tools and Utilities • Service Contract Center • Products and Services • Networking Solutions • Integration Utilities • Open Forum: Documentation
CiscoWorks Resources	Click this link and expand to view the following Network and Software details by clicking the corresponding sub links.
Third Party	Allows you to register your personal links.
Custom Tool	Allows you to register links in Custom Tool.

Adding Portlets From the Remote Server

You can access portlets from a remote server. You can also add such portlets to CiscoWorks LMS dashboards.

For instance, assume that you have installed one application in a different server and want to view the portlet details of the application from that server.

Before you connect to the remote server (to fetch the list of portlets) you must check whether the System Identity and password of the two servers (local and remote) are the same.

The remote servers System Identity username and password should be the same as those of the local server.

If the remote server is in the HTTPS mode (SSL mode), the remote server certificate should be imported.



Note

You cannot access LMS 4.0 portlets from a remote server that has LMS 3.2, or earlier installed.

To add portlets from a remote server:

Step 1

Click the Add Portlet icon at the top right corner of the CiscoWorks LMS page.

A popup window appears. Each section in this window contains a list of portlets.

You can expand and collapse the sections by clicking the arrows next to the section titles.

- Step 2** Click **CiscoWorks** and select **Others**.
A list of portlet names appear.
- Step 3** Click **Add** next to the Remote portlet that you wish to add.
The Remote portlet is displayed in CiscoWorks LMS Portal.
- Step 4** Click the Configuration icon.
- Step 5** To fetch the portlet from the remote server, enter a server name in the Server field, and click **Fetch**.
This fetches the portlet from a remote server.
- Step 6** Select the portlet from the Portlet drop-down list.
- Step 7** Click **Save** to view the portlet with the configured settings.
-

Adding RSS Portlet

Really Simple Syndication (RSS) is an XML-based format used to distribute Web content (such as news headlines). RSS allows web content publishers to create and disseminate the most current news headlines and URLs.

You can configure RSS in the CiscoWorks LMS application. You can create, add, modify any URL in the RSS portlet and view the details. You can also change the content and the title while configuring the RSS portlet.

To add the RSS portlet:

-
- Step 1** Click the Add Portlet icon at the top right corner of the CiscoWorks LMS page.
A popup window appears. Each section in this window contains a list of portlets.
You can expand and collapse the sections by clicking the arrows next to the section titles.
- Step 2** Click **Miscellaneous**.
The RSS portlet appears along with other portlets.
- Step 3** Click **Add** next to the RSS portlet.
The RSS portlet is displayed in CiscoWorks LMS Portal.
- Step 4** Click **Close** to close the popup window.
To configure RSS portlet, see [Configuring RSS](#).
-

Configuring RSS

To configure RSS portlet:

-
- Step 1** Go to CiscoWorks LMS page and add RSS portlet. For more information, see [Adding RSS Portlet](#).
- Step 2** Move the mouse over the title bar of the RSS portlet.
- Step 3** Click the Configuration icon and do the following:
- Enter one URL on each line.
 - Select the number of URLs to be displayed in the RSS portlet from the # of Items Per Channel drop-down list.
- For instance, if you have entered ten URLs in RSS portlet and if you want to view only two URLs, you can select **2** from the # of Items Per Channel drop-down list.
- Step 4** Click **Save** to view the portlet with the configured settings.
-

Adding IFrame Portlet

Intra Frame (IFrame) portlet enables you to open new or multiple pages inside the same browser window. You can change the content, title and the size of the IFrame portlet.

If you browse or check your mail regularly, you can have a portlet exclusively for this purpose. To do this you need to configure the URLs or websites within the IFrame portlet. You can also change the title, customize the URL, and the width and height of the portlet.

To add an IFrame portlet:

-
- Step 1** Click the Add Portlet icon at the top right corner of the CiscoWorks LMS page.
- A popup window appears. Each section in this window contains a list of portlets.
- You can expand and collapse these sections by clicking the arrows next to the section titles.
- Step 2** Click **Miscellaneous**.
- The IFrame portlet name appears along with other portlets.
- Step 3** Click **Add** next to the IFrame portlet name.
- The IFrame portlet is displayed in CiscoWorks LMS Portal.
- Step 4** Click **Close** to close the popup window.
- To configure the IFrame portlet, see [Configuring IFrame Portlet](#).
-

Configuring IFrame Portlet

To configure the IFrame portlet:

-
- Step 1** Go to the IFrame portlet and click the Configuration icon
- The Setup tab is displayed. Do the following:
- Enter the URL in the Source URL field.

For instance, you can enter the name of a website or any other URL to be displayed in the IFrame portlet as shown in [Figure 3-1](#).

For instance, you can enter the name of a website or any other URL to be displayed in the IFrame portlet.

Some websites do not work well with IFrames. If you add these web sites to IFrames they will take over the full browser window. This will hide the portal functions and make CiscoWorks inaccessible.

Figure 3-1 IFrame Portlet



Note

Cisco is not liable for the validity and support of any content or URL that is displayed inside the URL field. Some websites do not work well with IFrames. If you add these web sites to IFrames they will take over the full browser window. This will hide the portal functions and make CiscoWorks inaccessible.

- b. Select the Authenticate check box to authenticate.
- c. Select the authentication type from the Authentication Type drop-down list.
 - **Form** is the login form to enter your login credentials.
 - **Basic** is a pop-up or dialog box used to enter your login credential
- d. Select the form method from the Form Method drop-down list.
 - **Get** passes the variables in the URL.
 - **Post** puts the variables in session and is a more secure way to submit passwords.
- e. Enter the user name in the User Name field.
- f. Enter the password in the Password field.
- g. Enter the hidden variables in the Hidden Variable field.

If you would like to view a URL and that page requires some variables to be initialized, you can set these variables using the Hidden Variables option. You can enter the hidden variables you want to pass from one form to another without re-typing the information.

- h. Enter the HTML attributes in the HTML Attributes field.

The HTML attributes enable you to increase or decrease the frame border, height, space and width of a portlet. For instance, the normal height of a portlet is 300. If you want to increase the height you can enter the variables, accordingly.

- i. Click **Save** to save these settings.

Step 2 Click **Save** to save all of the settings.

If you encounter any problem after entering and saving the URL in the IFrame portlet follow this Recovery procedure:

Step 1 Click the URL <http://servername:portno/cwportal/c/portal/RemoveIframe>.

Step 2 Click the Remove IFrame Portlets button.

The IFrame portlet gets deleted.

Now you can create new IFrame portlets.

CiscoWorks Product Updates

You can view the recent updates and announcements of CiscoWorks products using CiscoWorks Product Updates.

Understanding Portlet Icons

Portlets are the basic user interface components that are managed and displayed in LMS dashboards. Each portlet contains six icons at the top right corner of the portlet.

The portlet icons appear only when you move the mouse over the top right corner of each portlet.

The icons that appear in a portlet are shown in [Table 3-9](#).

Move the mouse over each icon to view the names of the corresponding icons.

Table 3-9 Portlet Icons







Icons	Names	Function
	Change Title	Change the title of the portlet.
	Configuration	Enables you to set the configuration, such as the refresh time, and number of jobs displayed. This feature is not available for some of the portlets.
	Help	Opens the context-sensitive help for each portlet.
	Minimize	Hides and restores the content of a portlet.

Table 3-9 Portlet Icons (continued)

Icons	Names	Function
	Maximize	Enlarges the size of the portlet.
	Remove	Removes the portlet from the current view. This feature is not available for Functional View portlets.

Launching Portlets

You can launch a list of single and multi-instance (portlets that can be added more than once) portlets from the List Portlets page.

To access the List Portlets page:

Step 1 Enter the following URL in your web browser:

`http://server_name:portnumber/cwportal/PortletList`

Where *server_name* is the hostname of the server on which you installed LMS.

- If SSL is disabled, the default portnumber is 1741
- If SSL is enabled, the default portnumber is 443

A new page opens with a list of LMS Portlets.

The List contains all the portlets from the respective applications. All portlets are displayed as links.

Step 2 Click any of the portlet link to launch the corresponding portlet.

For instance, if you click the Critical Message Window link, a new pop-up window opens and the portlet appears.

Step 3 Close the new window to return to the home page.

Configuring Portlets

This section explains how to configure the portlets using the Configuration icon in CiscoWorks LMS portal.

You can configure the Refresh time for each portlet. In addition to the Refresh time, you can also configure details such as the alerts, collector number, exception period for a report for some of the portlets.

For example,

To configure the Refresh time:

Step 1 Click the Configuration icon.

Step 2 Select the minute and hour from the Refresh Every drop-down list to change the Refresh time.

The items in the portlet get refreshed at the changed Refresh time.

Step 3 Click **Save** to view the configured portlet with the changed Refresh time.



Note

To disable the Refresh time, uncheck the Auto Refresh check box. You can also click the Refresh icon displayed at the top right corner of the CiscoWorks LMS page to view the latest data in the portlet.

Changing the Title of a Portlet

You can change the title of the portlet using the Change Title icon that appears in the portlet. The Change Title icon appears only when you move the mouse over the top-right corner of the portlet.

To change the title of the portlet:

Step 1 Move the mouse over the top-right corner of a portlet to view the icons.

Step 2 Click the Change Title icon.

The Change Title portlet appears.

Step 3 Select the Use Custom Title check box.

The portlet name appears on the Portlet Title field.

Step 4 You can edit the Portlet Title field.

Step 5 Click **Save** to save all the changes.

Or

Click **Reset** to restore all fields and check boxes to their default values.

Changing the Portal Layout

You can organize the portlets into various columnar layouts as required.

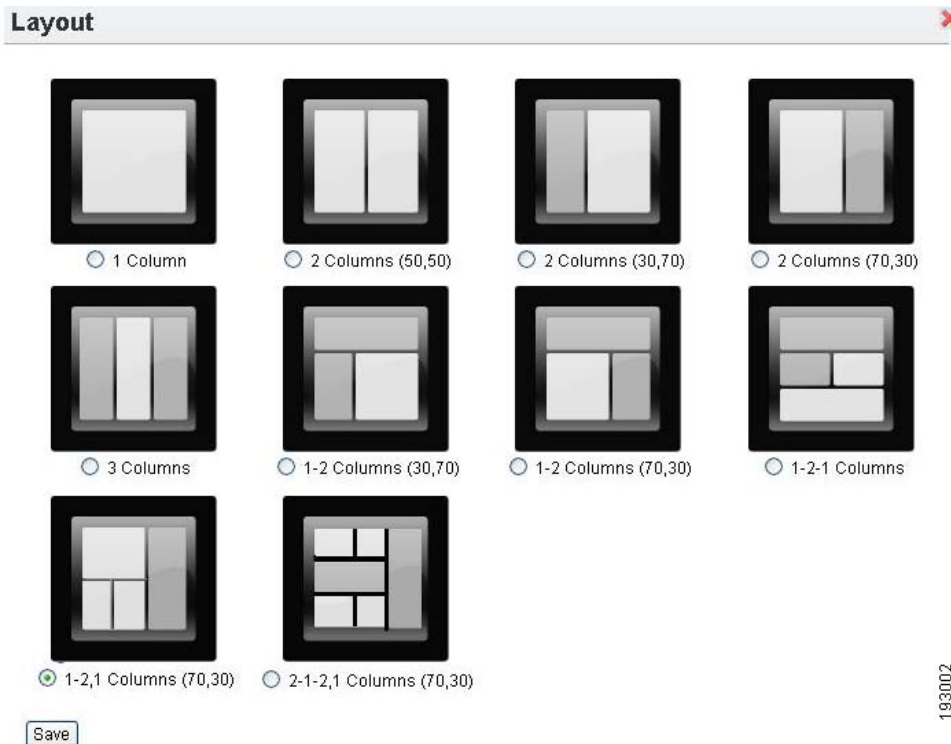
You can display the rows and columns in different layouts using the Change Layout icon displayed at the top right corner of the CiscoWorks LMS page.

To change the columnar layout of portlets:

Step 1 Click the Change Layout icon at the top right corner of the CiscoWorks LMS page.

A popup window appears.

Step 2 Select a layout option from the Layout window and click **Save**.



Step 3 Click the Close button to close the popup window.

[Table 3-10](#) lists the details of the column layouts.

Table 3-10 *Column Layout*

Column Layout	Description
1-Column	Displays one portlet in each row. Each portlet occupies the entire width of a row.
2-Columns (50/50)	Displays two portlets in each row. Each portlet occupies 50% of the row area.
2-Columns (30/70)	Displays two portlets in each row. The portlet on the left occupies 30% of the row area and the remaining 70% of the row area is occupied by the portlet on the right.
2-Columns (70/30)	Displays two portlets in each row. The portlet on the left occupies 70% of the row area and the remaining 30% of the row area is occupied by the portlet on the right.
3-Columns	Displays three portlets in each row. Depending on the content of the portlet, the portlets shrink or stretch automatically.

Table 3-10 Column Layout (continued)

Column Layout	Description
1-2 Columns (30/70)	<p>Displays one portlet in the top row.</p> <p>The rest of the portlets are displayed in the below row with the portlets on the left occupying 30% of the row area and the remaining 70% of the row area being occupied by the portlet on the right.</p>
1-2 Columns (70/30)	<p>Displays one portlet in the top row.</p> <p>The rest of the portlets are displayed in the below row with the portlets on the left occupying 70% of the row area and the remaining 30% of the row area being occupied by the portlet on the right.</p>
1-2-1 Columns	<p>Displays one portlet in each row at the top and bottom of the page.</p> <p>Two portlets in each row are displayed in the middle of the page.</p>
1-2, 1 Columns (70,30)	<p>Displays a combination of two columns.</p> <p>In the first column (70%) you can do the following:</p> <ul style="list-style-type: none"> • In the first half of the first column you can add a portlet. • In the second half of the first column you can add two portlets. <p>In the second column row (30%), you can add one portlet</p>
2-1-2,1 Columns (70,30)	<p>Displays two portlets in each row at the top and bottom of the page. This covers 70% of the page.</p> <p>One portlet is displayed in the middle of the page.</p> <p>The rest of the 30% of the page displays a single column and single portlets can be arranged column wise.</p>

**Note**

You can also drag and drop the portlets into different locations. While dragging, you must select the name of the portlet and drop only when the green arrows appear on both sides of the portlet.

Adding and Configuring Dashboards

You can perform the following operations:

- Add Dashboards (see [Add Dashboards](#))
- Set Dashboard Types (see [Set Dashboard Types](#))
- Hide Dashboards (see [Hide Dashboards](#))
- Copy Dashboards (see [Copy Dashboard Contents to a New Dashboard](#))
- Delete Dashboards (see [Delete Dashboards](#))
- Set Default Dashboards (see [Set Default Dashboard](#))

Add Dashboards

This section explains the procedure for adding a new dashboard for the following dashboard types:

- [My Dashboard](#)—User-defined dashboards accessible only to the user who created them
- [Public Dashboard](#)—User-defined dashboards accessible to all users
- [Default Dashboard](#)—Default dashboards accessible to all users

To add a new dashboard:

Step 1 Select **Manage Dashboards**.

The Dashboard Settings page appears.

Step 2 Select the LMS (or username) root node from the tree.

Step 3 Enter a name for the dashboard in the Name field.

Step 4 Click **Add Dashboard**.

A new dashboard is created. A new dashboard with the name you entered appears under the corresponding dashboard type.

Set Dashboard Types

You can add dashboards based on the types such as Portlet, URL and Embedded.

To select the dashboard type as portlet:

Step 1 Select **Manage Dashboards**.

The Dashboard Settings page appears.

Step 2 Select the LMS (or username) root node from the tree.

- a. Select **New-Dashboard**.
- b. Enter the name of the dashboard in the Name field.

- c. Select the dashboard type as **Portlet** from the Type drop-down list.
- d. Click **Add Dashboard**.

The new dashboard of the type Portlet gets added.

To select the dashboard type as Embedded:

Step 1 Select **Manage Dashboards**.

The Dashboard Settings page appears.

Step 2 Select the LMS root node from the tree.

- a. Select **New-Dashboard**.
- b. Enter the name of the dashboard in the Name field.
- c. Select the dashboard type as **Embedded** from the Type drop-down list.
- d. Click **Add Dashboard**.

The dashboard is added and appears in the tree.

Step 3 Click the embedded dashboard from the tree.

Step 4 Enter the URL and click **Save**.

The URL gets embedded within the dashboard.



Note The URL must be either http or https type.

To select the dashboard type as a URL:

Step 1 Select **Manage Dashboards**.

The Dashboard Settings page appears.

Step 2 Select the LMS root node from the tree.

- a. Select **New-Dashboard**.
- b. Enter the name of the dashboard in the Name field
- c. Select the dashboard type as URL from the Type drop-down list.
A URL field appears.
- d. Enter the URL in the URL field.
- e. Click **Add Dashboard**.

The URL is saved in the view.

Hide Dashboards

LMS allows you to hide the user-defined dashboards from the menu list.

To hide an existing user-defined dashboard:

-
- Step 1** Select **Manage Dashboards**.
The Dashboard Settings page appears.
- Step 2** Select the user-defined dashboard you want to hide from the tree.
The selected dashboard name appears in the Name field.
- Step 3** Select Hidden check box to enable this feature.
- Step 4** Click **Add Dashboard**.
The user-defined dashboard is saved with hide settings and the link to the dashboard will be removed from the My Menu list.
-

Copy Dashboard Contents to a New Dashboard

You can copy an existing dashboard. This allows you to create a new dashboard with the attributes of the original dashboard. However, you must name each dashboard with a unique name. You can modify the attributes of the new dashboard, as required.

To copy a dashboard:

-
- Step 1** Select **Manage Dashboards**.
The Dashboard Settings page appears.
- Step 2** Select the dashboard you want to copy to, from the tree.
The selected dashboard name appears in the Name field.
- Step 3** Select the dashboard you want to copy from the Copy Dashboard drop-down list.
When you copy an existing dashboard to a new dashboard, it will overwrite the contents of the previous dashboard.
For example, if you copy all the contents of a Configuration dashboard to Monitoring dashboard, the Monitoring dashboard contents will be overwritten by Configuration dashboard.
- Step 4** Click **Save** to save the changes.
-

Delete Dashboards

You can delete only user-defined dashboards. For instance, you create a dashboard and add contents into it as required and later delete it.

**Note**

You cannot delete system-defined dashboards.

The Default Dashboards (system-defined) are available by default with the application. These are Configuration, Device Status, Inventory, Monitoring, System, EnergyWise, and Identity.

To delete a dashboard:

Step 1 Select **Manage Dashboards**.

The Dashboard Settings page appears.

Step 2 Select the dashboard you want to delete from the tree.

The selected dashboard name appears in the Name field.

Step 3 Click **Delete** to delete the dashboard.

A message appears prompting you to confirm your decision.

Step 4 Click **OK** to confirm.

A message appears confirming that the dashboard has been deleted. The dashboard is permanently deleted after you click the Update button.

You can also delete dashboards by selecting the dashboards from **The Set the display order of dashboards** list box and click **Delete** (icon). See [Set Default Dashboard](#) for more information.

Deleting a Child Dashboard

You can delete a newly created Child dashboard.

To delete a Child dashboard:

Step 1 Select **Manage Dashboards**.

The Dashboard Settings page appears.

Step 2 Select the LMS dashboard node from the tree.**Step 3** Click **Children**.

The name of the Child dashboards appear.

Step 4 Select the Child dashboard to be deleted and click **Delete**.

A warning appears that the selected dashboard will be deleted when you click **Update** to apply the changes.

The Child dashboard is permanently deleted after you click **Update**.

Set Default Dashboard

You can set a dashboard to be shown by default whenever you login to LMS. This is done by reordering the dashboard list in My Menu using the Manage Dashboards option. The default dashboard can be viewed by all users.


Note

The default dashboard setup is applicable only for Public and Default Dashboards.

To set a default dashboard:

Step 1 Select **Manage Dashboards**.

The Dashboard Settings page appears.

Step 2 Select the dashboard node from the tree.

Step 3 Click **Display Order**.

The Set the display order of dashboards list box appears, displaying the list of dashboards.

Step 4 Select a dashboard from the list, and click Up Arrow or Down Arrow button to rearrange the dashboard.

Step 5 Click **Update** to apply the settings.

The dashboard that appears first in the list is set as the default dashboard. This dashboard is shown by default whenever you login to LMS.

Understanding the Search Bar

CiscoWorks LMS comes with a new search bar that can be accessed from across all pages. Using the new improved search, you can perform simple keyword and object-based search and the results are displayed in a pop-up window.

To perform a search:

Step 1 Select one of the following object types from drop-down list:

- **Device**—Search for devices by entering the display name, IP address, or host name of the device as the search input. For example, 55.1.222.1 or hostname of the device.

You can also use the wildcard character (*). For example, you can use 10.77.* to view all the devices starting with the IP address 10.77.

- **Jobs**—Search for jobs by entering the Job ID or Job description as the search input. For example, 1016, or 1026.

You can also use the wildcard character (*). For example, you can use 100*, or system* to view all jobs starting with 100, or system.

- **End Hosts**—Search for end hosts by entering MAC address, IP address, host name, or user name as the search input. For example, 01-36-6a-d7-02-05, 10.77.209.209, 10.77.209.209 or admin.

You can also use the wildcard character (*). For example, you can use 01-36-6a-d7-02-* to view all the devices starting with the MAC address 01-36-6a-d7-02-.

- Help—Search for help topics by entering the help text as the search input. For example, deploying templates.
- Tasks—Search for a task by entering the task name as the search input. For example, Troubleshooting or EnergyWise.

You cannot use wildcard character (*) for searching tasks.

Step 2 Enter the search input and click the continue icon.

A pop-up window appears, showing the first 20 results.

If there are more than 20 results, then a hyperlink (for example, Showing first 20 results of 300 records) shown in the pop-up window takes you to a global search results page the next 500 records.



Note

The search results for Help object are shown in a separate pop-up window.

See [Understanding Global Search Results Page](#) for more information.

Understanding Global Search Results Page

The Global Search results page shows a maximum of 500 search records for a search object. See [Understanding the Search Bar](#) for more information.

[Table 3-11](#) describes the Global Search results page for Device search.

Table 3-11 Global Search Results for Device Search

Column Name	Description
Display Name	Shows the display name of the device
IP Address	Shows the IP address of the device
Device Type	Shows the device type. For example Cisco 3640 Multiservice Platform
Host Name	Shows the host name of the device

[Table 3-12](#) describes the Global Search results page for Task search.

Table 3-12 Global Search Results for Task Search

Column Name	Description
Display Name	Shows the display name of the task
Task Description	Shows a description of the task

Table 3-13 describes the Global Search results page for Jobs search.

Table 3-13 Global Search Results for Jobs Search

Column Name	Description
Job ID	Shows the Job ID
Job Description	Describes the job. For example, System Inventory Collection job.
Job Type	Shows the job type.
Job Status	Shows the job status. For example, scheduled.

Table 3-14 describes the Global Search results page for End Host search.

Table 3-14 Global Search Results for End Host Search

Column Name	Description
MAC Address	Shows the MAC address of the end host.
Host IP Address	Shows the IP address of the end host.
Host Name	Shows the display name of the end host.
User Name	Shows the user name of the end host.

Understanding the Fault Bar

The new Fault bar floats across all pages in LMS. The Fault bar allows you to view the number of faults and events in your network.

The following fault types are available:

- Critical—Shows the number of faults of type critical in your network
- Warning—Shows the number of faults of type warnings in your network
- Info—Shows the number of faults of type information in your network

Click the fault icon (Critical, Warning, Info) to know more about these faults. This takes you to the Device Fault Summary page in LMS, where you can know the faults and events in your network.

See *Monitoring and Troubleshooting with CiscoWorks LAN Management Solution 4.0* for more information.

Adding Links to Favorites

LMS allows you to add the frequently used task links (URL link) as favorites.

To add links to favorites:

-
- Step 1** Go to CiscoWorks LMS page.
- Step 2** Click the favorite icon from the toolbar.
- The Add to favorites pop-up menu appears, displaying the list of links added to favorites.
- Step 3** Click **Add Favorite** from the pop-up menu to add the current page URL to the favorites list.
- The Add to favorites dialog box appears, displaying the current page name and the URL link.
- Step 4** Click **Add** to bookmark the current page to favorites list.
-

Navigating Legacy Menu

You can perform LMS functions by using the legacy LMS 3.x navigation menus.

To access the legacy navigation path:

-
- Step 1** Go to CiscoWorks LMS page.
- Step 2** Click the legacy icon from the toolbar.
- The legacy menu appears displaying LMS 3.x links to access LMS features.
- See *Navigation Guide for CiscoWorks LAN Management Solution 4.0* for more information.
-

Using Online Help

The Online help provides procedural and conceptual information for the functions in LMS. The Online help also contains:

- A search engine—Allows you to search the topics in Online help, based on keywords.
- An index—Contains typical network tasks.
- A dropin list—Contains functional help modules.
- View PDF—View the user guide in PDF format.
- A glossary.

To access Online help, click the **Help** link on the top-right corner.

This opens a window that displays help contents. From this window, you can access help for device packages and for the following LMS functions:

- Getting Started
- Monitor

- Inventory
- Configuration
- Reports
- Admin
- Work Centers

To view the help for a functional module (For example, Configuration), use the dropin list on the left and select the specific functional module help.



CHAPTER 4

Dashboards in LMS

This chapter provides information on LMS dashboards.

Dashboards provide you with a quick snapshot of specific functions in LMS. The following functional dashboards are available in LMS:

- [Monitoring Dashboard](#)
- [Identity Dashboard](#)
- [EnergyWise Dashboard](#)
- [Inventory Dashboard](#)
- [Configuration Dashboard](#)
- [Device Status Dashboard](#)
- [System Dashboard](#)

Monitoring Dashboard

The Monitoring dashboard in LMS shows the following portlets:

- Device Availability
- Interface Availability
- High Severity Alerts
- TOP-N Interface Discards
- TOP-N Memory Utilization
- TOP-N CPU Utilization
- TOP-N Interface Utilization
- TOP-N Interface Errors
- Live - Graph It
- Histo - Graph It
- N-Hop View
- Performance Threshold Information
- IPSLA Violation Summary
- Fault Events Summary

- Syslog Summary
- Syslog Alerts
- Syslog Messages
- TOP-N Syslog Sender

See *Monitoring and Troubleshooting with CiscoWorks LAN Management Solution 4.0* for more information.

Identity Dashboard

The Identity dashboard in LMS shows the following portlets:

- Identity - Authenticated User
- Identity - 802.1x Agentless User
- Identity - Authorization Trend Portlet
- Identity - Security Mode Distribution
- Identity - Authentication Trend
- Job Approval
- User Tracking Summary

See *Technology Work Centers in CiscoWorks LAN Management Solution 4.0* for more information.

EnergyWise Dashboard

The EnergyWise dashboard in LMS shows the following portlets:

- EnergyWise - End Point Groups
- EnergyWise - Total Savings Graph
- EnergyWise - Policy Override
- Job Approval
- EnergyWise - Power Consumption Graph
- EnergyWise - Current Power Consumption
- EnergyWise - Savings Trend Graph

See *Technology Work Centers in CiscoWorks LAN Management Solution 4.0* for more information.

Inventory Dashboard

The Inventory dashboard in LMS shows the following portlets:

- Hardware Summary
- Software Summary
- Device Change Audit
- User Tracking Summary

- Device Discovery Summary
- Supported Device Finder

See *Inventory Management with CiscoWorks LAN Management Solution 4.0* for more information.

Configuration Dashboard

The Configuration dashboard in LMS shows the following portlets:

- Hardware Summary
- Software Summary
- Config Protocol Summary
- Discrepancies
- Best Practices Deviation
- Device Change Audit
- Job Information Status
- Job Approval
- Syslog Alerts

See *Configuration Management with CiscoWorks LAN Management Solution 4.0* for more information.

Device Status Dashboard

The Device Status dashboard in LMS shows the following portlets:

- VRF Collector Summary
- Device Performance Management Summary
- Device Discovery Summary
- Job Information Status
- Config Protocol Summary
- Device Credentials Verification Error Summary
- Supported Device Finder
- Collection Summary
- Job Approval
- Audit Trail Information

See *Inventory Management with CiscoWorks LAN Management Solution 4.0* for more information.

System Dashboard

The System dashboard in LMS shows the following portlets:

- Job Information Status
- Critical Message Window
- Process Status
- System Backup Status
- User Login Information
- Log Space Usage
- Syslog Collectors Information
- Device Discovery Summary
- Device Credentials and AAA Information

See *Administration of CiscoWorks LAN Management Solution 4.0* for more information.



CHAPTER 5

Configuring Multiserver Setup

This chapter provides information for configuring multiserver setup in LMS.

It explains:

- [Viewing the Current Server Settings](#)
- [Converting the Server as Master or as Standalone](#)
- [Converting the Server as Slave](#)
- [Changing the Server Mode to DCR Standalone, Master and Slave](#)
- [Changing the Server Mode to SSO Standalone, Master and Slave](#)
- [Adding Peer Server Certificates](#)
- [Setting up System Identity Account](#)



Note

By default, the LMS server is in Standalone mode.

Viewing the Current Server Settings

This section provides information on the CiscoWorks LMS Server settings currently configured.

[Table 5-1](#) provides the description of the fields in the Current Server Settings table.

Table 5-1 *Current CiscoWorks LMS Server Settings*

Column	Description
Hostname or IP Address	Hostname or IP Address of the CiscoWorks server
Server Display Name	Display name you have set up for the LMS server.
Protocol	Protocol of the server. This can be HTTP or HTTPS.
Port	Port number of the CiscoWorks server. For example, 1741
DCR Mode	DCR mode of the server. DCR mode can be Master, Slave, or Standalone.
SSO Mode	SSO mode of the server. SSO mode can be Master, Slave, or Standalone.

Converting the Server as Master or as Standalone

To convert the server as Master or as Standalone, you need to:

- Change the Device Credential Repository (DCR) Mode (See [Changing the Server Mode to DCR Standalone, Master and Slave](#))
- Change the Single Sign-On (SSO) Mode (See [Changing the Server Mode to SSO Standalone, Master and Slave](#))

For information about DCR Master, DCR Slave and DCR Standalone modes, see the section DCR Architecture in *Inventory Management with CiscoWorks LAN Management Solution 4.0*.



Note

By default, the LMS server setup is in Standalone mode.

Converting the Server as Slave

To convert the server as Slave, you need to:

1. Configure a Master server (this is a prerequisite). Hostname of the master server should be DNS resolvable.
2. Configure Peer Server Certificate on master and slave (See [Adding Peer Server Certificates](#))
3. Configure System Identity setup on master and slave. Ensure the System Identity username and password are the same across all servers (See [Setting up System Identity Account](#))
4. Change Device Credential Repository Mode to slave (See [Changing the Server Mode to DCR Standalone, Master and Slave](#))
5. Change Single Sign-On Mode to slave (See [Changing the Server Mode to SSO Standalone, Master and Slave](#))

For information about DCR Master, DCR Slave and DCR Standalone modes, see the section DCR Architecture in *Inventory Management with CiscoWorks LAN Management Solution 4.0*.

Changing the Server Mode to DCR Standalone, Master and Slave

This section explains the following DCR modes:

- [Changing the Mode to Standalone](#)
- [Changing the Mode to Master](#)
- [Changing the Mode to Slave](#)

Changing the Mode to Standalone

Step 1 Go to Multiserver configuration workflow from the Getting Started Assistant pane.

Step 2 Click **Multiserver Configuration**.

The Multiserver Configuration page appears, showing the procedure to change the DCR mode (See Step 1: Change **Device Credential Repository Mode**).

- Step 3** Click **Device Credential Repository Mode** to change the DCR mode.
The DCR pop-up window appears.
- Step 4** Select the **Standalone** radio button.
- Step 5** Click **Apply** to change mode.
The default DCR mode is Standalone.
-

Changing the Mode to Master

- Step 1** Go to Multiserver Configuration workflow from the Getting Started Assistant pane.
- Step 2** Click **Multiserver Configuration**.
The Multiserver Configuration page appears, showing the procedure to change the DCR mode (See Step 1: Change **Device Credential Repository Mode**).
- Step 3** Click **Device Credential Repository Mode** to change DCR mode.
The DCR pop-up window appears.
- Step 4** Select the **Master** radio button.
- Step 5** Click **Apply** to change mode.
-

Changing the Mode to Slave

- Step 1** Go to Multiserver Configuration workflow from the Getting Started Assistant pane.
- Step 2** Click **Multiserver Configuration**.
The Multiserver Configuration page appears, showing the procedure to change the DCR mode (See Step 1: Change **Device Credential Repository Mode**).
- Step 3** Click **Device Credential Repository Mode** to change DCR mode
The DCR pop-up window appears.
- Step 4** Select the **Slave** radio button.
- Step 5** Enter the hostname of the Master in the Master field.
This hostname should exactly match the Hostname field in the Master's Self Signed Certificate.
- Step 6** Specify the SSL port of the master. Default is 443.
- Step 7** Select **Inform current slave of new master hostname** check box only if you want to change the mode from Master to Slave.
If you select this check box, all the slaves of the Master (whose mode you currently changed to Slave) will be informed of the new master hostname. That is, they will become the slaves of the new Master.
- Step 8** Select the Add new devices to Master check box to add the devices in Slave to the new Master.
If the devices are already available in the new Master, they will be discarded.

Step 9 Click **Apply**.

A warning message appears when the Master server has the earlier version of Common Services.

Step 10 Click **OK** to change the mode to Slave.

To cancel the change of mode, click **Cancel**.

**Note**

You must restart the daemon manager after the mode change to Slave is complete.

Changing the Server Mode to SSO Standalone, Master and Slave

The LMS server can be configured for Single Sign-On (SSO). It can also be configured to be in Standalone mode (Normal mode, without SSO).

**Note**

By default, the LMS server setup is in Standalone mode.

When the server is configured for SSO, it can either be in:

- Master mode—The SSO Authentication Server does the authentication and sends the result to the Regular Server.

Change the SSO mode to Master, if login is required for all SSO regular servers. Login requests for all the SSO regular servers will be served from the Master.

- Slave mode—SSO Regular server for which authentication is done at the Master.

While logging into regular server, if the authentication server is not reachable, the following message appears:

```
SSO unreachable
```

Only one server is configured to be in the Master mode. All other servers are configured as Slaves. If the server is configured as an SSO Regular server (Slave), you should provide the following details:

- Master server name

The Master server name must be DNS resolvable. If you change the name of the SSO Master server, in the `/etc/hosts` file, you must restart Daemon Manager for the name resolution to reflect in the Slave.

When you have configured more than one SSO Slave server for a SSO Master server, you must ensure to enter either the fully qualified domain name or hostname of the Master consistently in all the Slave servers.

Authentication would not occur if you enter the domain name of Master in one SSO Slave and hostname of the same Master server in another SSO Slave.

- Login Port of the Master (443)

This section explains:

- [Changing the SSO Mode to Standalone](#)
- [Changing the SSO Mode to Master](#)
- [Changing the SSO Mode to Slave](#)

Changing the SSO Mode to Standalone

- Step 1** Go to Multiserver Configuration workflow from the Getting Started Assistant pane.
 - Step 2** Click **Multiserver Configuration**.
The Multiserver Configuration page appears, showing the procedure to change the SSO mode (See Step 2: Change **Single Sign-On Mode**).
 - Step 3** Click **Single Sign-On Mode** to change SSO mode
The Single Sign-On Setup pop-up window appears.
 - Step 4** Select **Standalone (Normal)** radio button.
 - Step 5** Click **Apply**.
-

Changing the SSO Mode to Master

- Step 1** Go to Multiserver Configuration workflow from the Getting Started Assistant pane.
 - Step 2** Click **Multiserver Configuration**.
The Multiserver Configuration page appears, showing the procedure to change the SSO mode (See Step 2: Change **Single Sign-On Mode**).
 - Step 3** Click **Single Sign-On Mode** to change SSO mode
The Single Sign-On Setup pop-up window appears.
 - Step 4** Select **Master (SSO Authentication Server)** radio button.
 - Step 5** Click **Apply**.
-

Changing the SSO Mode to Slave

- Step 1** Go to Multiserver Configuration workflow from the Getting Started Assistant pane.
 - Step 2** Click **Multiserver Configuration**.
The Multiserver Configuration page appears, showing the procedure to change the SSO mode (See Step 2: Change **Single Sign-On Mode**).
 - Step 3** Click **Single Sign-On Mode** to change SSO mode.
The Single Sign-On Setup pop-up window appears.
 - Step 4** Select **Slave (SSO Regular Server)** radio button.
 - Step 5** Enter the Master server name and port number.
If you select the Slave mode, ensure that you specify the Master server name and port. The default port is 443. The server configured as Master (or Authentication Server) should be DNS resolvable.
 - Step 6** Click **Apply**.
-

Adding Peer Server Certificates

You can add the certificate of another CiscoWorks Server into its trusted store. This will allow one CiscoWorks Server to communicate to another using SSL. If a CiscoWorks Server needs to communicate to another CiscoWorks Server, it must possess the certificate of the other server. You can add certificates of any number of peer CiscoWorks Servers to the trusted store.

You must add peer server certificates if CiscoWorks Servers are configured with Self-Signed Certificates. If the certificates have been signed by popular CAs such as Verisign, and GlobalSign this is not compulsory. However, we recommend that you add peer server certificates to avoid any possible problems with SSL communication.

You can use this option from the client browser and from a browser session on the server where CiscoWorks Server is installed.

To add peer CiscoWorks Server certificates:

-
- Step 1** Go to **Admin > Trust Management > Multiserver > Peer Server Certificate Setup**.
The Peer Server Certificate page appears with a list of certificates imported from other servers.
 - Step 2** Click **Add**.
 - Step 3** Enter the IP address/hostname of the peer CiscoWorks Server in the corresponding fields.
If you specify a server name, it must be entered in DNS. Otherwise specify the IP Address.
 - Step 4** Enter the value of the SSL (HTTPS) Port of the peer CiscoWorks Server. The default SSL(HTTPS) Port of the peer CiscoWorks Server is 443.
 - Step 5** Click **OK**.
-

See *Administration of CiscoWorks LAN Management Solution 4.0* for more information.

Setting up System Identity Account

Communication between multiple CiscoWorks Servers is enabled by a trust model based on certificates and shared secrets. System Identity setup helps you to create a trust user on servers that are part of a multi-server setup. This user enables communication among servers that are part of a domain.

There can only be one System Identity User for each machine.

The System Identity User you configure must be a Peer Server User. The System Identity User you create must be a local user with all privileges.

You can configure the System Identity User either with the predefined Super Admin role, or with a custom role created with all privileges. If you change the System Identity User later, you must ensure that you add the local user with all privileges in CiscoWorks.

CiscoWorks installation program allows you to have the admin user configured as the default System Identity User.

For the admin user to work as a System Identity User, the same password should be configured on all machines that are part of the domain, while installing CiscoWorks on the machines part of that domain. If this is done, the user admin serves the purpose of System Identity user. See *Installing and Migrating With LAN Management Solution 4.0* for details.

If you create a System Identity User, the default System Identity User, admin, is replaced by the newly created user.

While you create the System Identity User, LMS checks whether:

- The user is a Local User with all privileges. If the user is not present, or if the user does not have all privileges, an error message appears.
- The System Identity User is also a Peer Server User. If not, the user will be made a Peer Server User.

For peer to peer communication to work in a multi-server domain, you have to configure the same System Identity User on all the machines that are part of the domain.

For example, if S1, S2, S3, S4 are part of a domain, and you configure a new System Identity User, say Joe, on S1, you have to configure the same user, Joe, with the same password you specified on S1, on all the other servers, S2, S3, and S4, to enable communication between them.

To add a System Identity user:

-
- Step 1** Select **Admin > Trust Management > Multiserver > System Identity Setup**.
 - Step 2** Enter the username in the Username field.
 - Step 3** Enter the password in the Password field.
 - Step 4** Re-enter the password in the Verify field.
 - Step 5** Click **Apply**.
-

SSO uses the System Identity User password as the secret key to provide confidentiality and authenticity between Master and Slave.

The System Identity User password you specify in Master and Slave should be the same. We recommend that you have the same user name and password across Master and Slave.



CHAPTER 6

Configuring E-mail, Cisco.com and Proxy Settings

This chapter guides you on configuring the following settings using the Getting Started workflow:

- [E-mail Settings](#)
- [Cisco.com Settings](#)
- [Proxy Settings](#)

E-mail Settings

This section explains the configuration of E-mail settings on the CiscoWorks LMS server.

To configure E-mail settings:

-
- Step 1** Select **E-mail** in System Settings workflow.
- Step 2** Enter the following details:
- **SMTP Server**—System-wide name of the SMTP server used by CiscoWorks LMS functions to deliver reports. The default server name is localhost.
 - **Admin E-mail ID**—CiscoWorks Administrator E-mail ID. This e-mail address is used as the From Address in all mails sent from the CiscoWorks LMS server. There is no default E-mail ID.
 - **Enable E-mail Attachment**—Allows you to enable E-mail attachments in the mails sent from the CiscoWorks LMS server. This option helps you to attach PDF or CSV reports with the E-mail after the scheduled jobs have completed. This option is enabled by default.
 - **Maximum Attachment Size**—Maximum size of the E-mail attachments that are allowed to be sent from the CiscoWorks LMS server. You can specify the attachment size in KB or MB.
- Step 3** Click **Apply** to save E-mail settings.
-

Cisco.com Settings

This section explains the configuration, validation, and saving of Cisco.com login credentials on the CiscoWorks LMS server. Setting up Cisco.com login credential is optional.

To configure Cisco.com settings:

-
- Step 1** Select **Cisco.com** in System Settings workflow.
- Step 2** Enter the following details:
- **User Name**—Enter the Cisco.com login user name.
 - **Password**—Enter the password for the Cisco.com login user name.
 - **Confirm Password**—Re-enter the Cisco.com password in this field.
- Step 3** Click **Test** to validate the Cisco.com login credentials.
- Step 4** Click **Apply** to save the Cisco.com login credentials.
-

Proxy Settings

This section explains the entry and saving of proxy server settings on the CiscoWorks LMS server.

To configure proxy server settings:

-
- Step 1** Select **Proxy** in System Settings workflow.
- Step 2** Enter the following details:
- **Host Name and IP Address**—Enter the proxy server host name or IP address
 - **Port**—Enter the port number for accessing the proxy server
 - **User Name**—Enter user name for accessing the proxy server
 - **Password**—Enter the password for accessing the proxy server
 - **Confirm Password**—Re-enter the password.
- Step 3** Click **Test** to validate proxy server credentials.
- Step 4** Click **Apply** to save the proxy server settings.
-



CHAPTER 7

Updating Software and Device Packages and Migrating Data

This chapter guides you on viewing and downloading software and device package updates in LMS 4.0, and also migrating data from the current or earlier versions of LMS to LMS 4.0.

It explains:

- [Updating Software and Device Packages](#)
- [Understanding the Procedure for Migrating Data](#)

Updating Software and Device Packages

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 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 IDU have to be installed based on the installation instructions in the respective Readme files.

The Getting Started workflow does not support installation and uninstallation of software updates.

For downloads from Cisco.com to work, you should have access to Cisco.

This section explains the following:

- [Viewing Software and Device Packages Installed](#)
- [Viewing Scheduled Job Details](#)
- [Scheduling Software Updates and Device Package Downloads](#)

For more information, see *Administration of CiscoWorks LAN Management Solution 4.0*.

Viewing Software and Device Packages Installed

The Software and Device Updates workflow in the Getting Started wizard describe the software updates and device packages currently installed on LMS. You can also view the number of software updates and device packages available for download on Cisco.com.

- [Table 7-1](#) describes the fields in Software Updates Download table.
- [Table 7-2](#) describes the fields in Device Package Download table.

Table 7-1 *Details of Software Updates Download*

Column Name/Button	Description
Product Name	Name of the product. For example, LAN Management Solution.
Installed Version	Product version currently installed. For example, 4.0
Available Version	Product version available for download on Cisco.com. For example, 4.0.1
Schedule Download (Button)	<p>Click to schedule software updates download.</p> <p>The Schedule Update pop-up window appears, where you enter the following details:</p> <ul style="list-style-type: none"> • Destination Location • Job Details <p>See Scheduling Software Updates and Device Package Downloads for more information.</p>

Table 7-2 *Details of Device Package Download*

Column Name/Button	Description
Package Name	Name of the package installed. For example, LAN Management Solution.
Installed Package Count	Total number of packages currently installed. For example, 300.
Available Package Count	Total number of packages available for download on Cisco.com. For example, 50
Schedule Download (Button)	<p>Click to schedule device package download.</p> <p>The Schedule Update pop-up window appears, where you enter the following details:</p> <ul style="list-style-type: none"> • Destination Location • Job Details <p>See Scheduling Software Updates and Device Package Downloads for more information.</p>

Viewing Scheduled Job Details

The Software and Device package workflow in Getting Started shows the details of jobs scheduled for downloading software updates and device packages. [Table 7-3](#) describes the fields in the Device and Software Job Details table.

Table 7-3 *Device and Software Job Details*

Column/Button	Description
ID	Unique ID assigned to the job by the system, when the job is created. For periodic jobs such as Daily, and Weekly, the Job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the Job ID 1001. You can view the job details by clicking on the hyperlink.
Type	Type of job scheduled for download (Schedule device download/Software update)
Status	Status of the scheduled job (Success or Failed).
Description	Description of the job provided by the job creator.
Owner	User who scheduled the job.
Start Time	Date and time at which the job was scheduled.
End Time	Date and time when the job completed.

Table 7-3 Device and Software Job Details

Column/Button	Description
Scheduled Type	<p>Type of schedule for the job (once/periodic).</p> <p>Note The schedule is once for software update jobs and periodic for device package download jobs.</p> <p>The following periodic job schedule options are available for device package downloads.</p> <ul style="list-style-type: none"> • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the specified day of the week and at the specified time. • Monthly—Runs monthly on the specified day of the month and at the specified time. <p>For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete.</p> <p>For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10:00 a.m. November 1 job has not been completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.</p>
Filter (Button)	<p>Click Filter. Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click Go to filter details.</p> <p>The following Filter By options are available:</p> <ul style="list-style-type: none"> • ID—Select ID and enter the Job ID • Type—Select Type and enter the Type (Schedule device download or Software update) • Status—Select Status and enter the status (Failed, Success) • Description—Select Description and enter the complete description • Owner—Select Owner and enter the user who created the job • Start Time—Select Scheduled At and enter the date and time • End Time—Select Completed At and enter the date and time • Schedule Type—Select Schedule Type and enter the type of schedule (once, periodic)

Scheduling Software Updates and Device Package Downloads

You can schedule a job to download Software updates and Device Packages from Cisco.com.

To schedule a job:

- Step 1** Select Software and Device Updates workflow from the Getting Started Assistant pane.
- Step 2** Go to:
- Software Updates table and click **Schedule Download** for scheduling Software updates job.
 - Device Package Download table and click **Schedule Download** for scheduling device package download job.

The Schedule Update pop-up window appears, where you enter the following:

- Destination Location
- Job Details

Table 7-3 describes the fields in the Schedule Update pop-up window.

Table 7-4 Schedule Update Field description

Fields/Options	Description
Destination Location	Either: <ul style="list-style-type: none"> • Enter the path to download Software updates or device packages. Or <ul style="list-style-type: none"> • Click Browse to locate and select the directory for downloading the software updates or device packages.
Job Details	
Run Type	Select the frequency at which the job should be run: <ul style="list-style-type: none"> • Once—Runs once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the specified day of the week and at the specified time. • Monthly—Runs monthly on the specified day of the month and at the specified time. (A month comprises 30 days). For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not been completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3. <p>Note The schedule for Software Update Download job runs only once. The other schedule options (Daily, Weekly and Monthly) are not available for Software Update Download jobs.</p>
Job Description	Enter the Job Description. Enter unique descriptions to help you identify the jobs easily. This is mandatory.

Table 7-4 Schedule Update Field description

Fields/Options	Description
E-mail	Enter e-mail addresses to which the job sends messages when the job has run. You can enter multiple e-mail addresses separated by commas.
Start Date	Click the calendar icon to select the start date.
Start Time	Set the start time by selecting the hour (HH) and minute (MM) from the drop-down list.

Step 3 Click **Apply**.

A notification message appears along with the Job ID. The newly created job appears in the Device and Software Job Details pane. See [Viewing Scheduled Job Details](#) for more information.

Understanding the Procedure for Migrating Data

Migration is the process of carrying over data from an earlier or same version of LMS to a newer or the same version of LMS.

This section provides an overview of migrating data in CiscoWorks LMS 4.0.

Migration involves:

1. Backing up the LMS data
2. Installing the newer version of LMS
3. Restoring the backed up data

LMS 4.0 does not support direct upgrade from the earlier versions of LMS.

The following LMS migration paths are applicable:

- LMS 4.0 to LMS 4.0
- LMS 3.2 to LMS 4.0
- LMS 3.1 to LMS 4.0
- LMS 3.0.1 to LMS 4.0
- LMS 3.0 to LMS 4.0
- LMS 2.6 SP to LMS 4.0
- LMS 2.6 to LMS 4.0

**Note**

You need to do a fresh install of LMS 4.0 and then perform data migration.

You can use the `restorebackup.pl` script to restore the LMS data you have backed up.

For a successful restoration of backed up data, ensure that all services and processes are up and running. Stop the daemons and then run `restorebackup.pl`.

To run `restorebackup.pl`, go to command prompt and run `restorebackup.pl`.

- On Solaris:

```
NMSROOT/bin/perl NMSROOT/bin/restorebackup.pl -d <Backup_Directory>
```

- On Windows:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl -d <Backup_Directory>
```

where, NMSROOT is the CiscoWorks installation directory.

Backup_Directory is the directory where the backup archive is located.

For more information on data migration, see *Installing and Migrating to CiscoWorks LAN Management Solutions 4.0*.



CHAPTER 8

Checking Protocol, Security, Backup and Authentication Settings

This chapter guides you on setting up the following using the Getting Started workflow:

- [RCP and SCP Settings](#)
- [Browser Server Security Settings](#)
- [Backup Settings](#)
- [Authentication Settings](#)

RCP and SCP Settings

This section explains the setting up of RCP and SCP credentials on the CiscoWorks LMS server.

To setup RCP and SCP:

-
- Step 1** Select **RCP and SCP** in System Settings workflow.
- Step 2** Enter the following details:
- **RCP User**—Name used by 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 the 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 protocol. 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**—Re-enter the SCP password in this field.
- Step 3** Click **Apply** to save the RCP and SCP settings.
-

Browser Server Security Settings

CiscoWorks LMS provides secure access between the client browser and the management server. This section explains you the enabling or disabling of the https security mode in browser and server.

Step 1 Select **Browser Server Security Mode** in System Settings workflow

Step 2 Select either:

- **Enable**—To change the settings to https mode.

Or

- **Disable**—To change the settings to non-secure http mode.

Step 3 Click **Apply** to save the security mode settings.

A pop-up message appears asking you to restart the Daemon process when you change the security settings.

Backup Settings

This section explains the configuration and scheduling of backup on the CiscoWorks LMS server.

To configure Backup settings:

Step 1 Select **Backup** in System Settings workflow.

Step 2 Enter the appropriate information in the following fields:

Table 8-1 Backup Settings

Field	Description
Backup Settings	
Backup Directory	Location of the backup directory. We recommend that your target location be on a partition other than the CiscoWorks installation location. The backup directory name should not contain any special characters.
Generations	Maximum number of backups to be stored in the backup directory.

Table 8-1 Backup Settings

Field	Description
Scheduler	
Run Type	<p>Select the backup schedule:</p> <ul style="list-style-type: none"> • Daily—The database is backed up every day at the time specified. • Weekly—The database is backed up once a week on the day and time specified. Select a day from the Day of week list. • Monthly—The database is backed up once a month on the day and time specified. Select a day from the Day of month list. <p>You cannot schedule more than one backup at a time. The new schedule overwrites the previous schedule, if any.</p>
E-mail	<p>Enter a valid E-mail ID in this field.</p> <p>You can enter multiple E-mail IDs separated by commas.</p>

Step 3 Click **Apply** to save the backup configuration settings.

Authentication Settings

This section explains the authentication login modules in LMS. Login modules define how authorization and authentication are performed. You can change the current authentication modules to any of the available list of login modules.

To change the authentication module:

Step 1 Select **Authentication Mode** in System Settings workflow.

The default authentication module in LMS is CiscoWorks Local.

You can change to any of the following authentication login modules:

- **CiscoWorks Local**—This login module is the default authentication module in LMS.
- **IBM SecureWay Directory**—This login module implements Lightweight Directory Access Protocol (LDAP). Before a user can login, the user account is set up in the LDAP server.
- **KerberosLogin**—This login module provides strong authentication for client/server applications by using secret-key cryptography.
- **Local NT System**—This login module is available only on Windows.
- **Local Unix System**—This login module is available only on Solaris.
- **MS Active Directory**—This login module implements Lightweight Directory Access Protocol (LDAP). Before a user can login, the user account is set up in the LDAP server.

- **Netscape Directory**—This login module implements Lightweight Directory Access Protocol (LDAP). Before a user can login, the user account is set up in the LDAP server.
- **RADIUS**—This login module connects to the RADIUS server to validate the user account.
- **TACACS+**—This login module connects to a TACACS server to validate the user account.

Step 2 Select the appropriate login module.

Step 3 Click **Apply** to save the authentication settings.



CHAPTER 9

Managing User Roles and Users in LMS

This chapter explains the following:

- [Managing Roles](#)
- [Managing Users](#)

Managing Roles

A role is a collection of privileges that dictate the type of system access you have. The Manage User Roles workflow allows you to add, edit, copy and delete user-defined roles in LMS. You can also set default user roles.

This section explains:

- [Creating User Roles](#)
- [Modifying User Roles](#)
- [Copying User Roles](#)
- [Deleting User Roles](#)
- [Setting Default Roles](#)



Note

Unicode character (U+2713) is not supported in Windows XP. If you see any strange character instead of a tick mark in the UI, you can use the DejaVu font set which supports the Unicode character(U+2713).

You can view the list of default fonts supplied with Windows XP at:
<http://www.microsoft.com/typography/fonts/product.aspx?PID=135>

Creating User Roles

To create a user role:

Step 1 Select User Management workflow from the Getting Started Assistant pane.

The following User Management tasks are shown:

- Manage Roles (see [Managing Roles](#))
- Manage Users (see [Managing Users](#))

Step 2 Click **Manage Roles**.

The Manage Roles page appears.

[Table 9-1](#) describes the Manage Roles pane.

Table 9-1 *Manage Roles Pane Description*

Column/Buttons	Description
Role	Lists the following user roles in LMS: <ul style="list-style-type: none"> • Help Desk—Can access network status information only. Can access persisted data on the system and cannot perform any action on a device or schedule a job which will reach the network. • Network Operator—Can perform all Help Desk tasks. Can perform tasks related to network data collection. Cannot perform any task that requires write access on the network. • Approver—Can approve all tasks. • Network Administrator—Can perform all Network Operator tasks. Can perform tasks that result in a network configuration change. • System Administrator—Can perform all CiscoWorks system administration tasks. • Super Admin—Can perform all CiscoWorks operations including the administration and approval tasks.
Description	Describes the role.
Default Role	The default role assigned to the user. Guest is the default role assigned for users who are authenticated by an alternative service and who are not in the local database.
Add (button)	Click Add to add a new role and assign LMS tasks to the role.
Edit (button)	Select an existing role and click Edit to modify the user-defined role and the LMS tasks assigned to the role.
Delete (button)	Select an existing role and click Delete to delete the user-defined role from LMS.
Filter (button)	Click Filter . Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click Go to filter details. The following Filter By options are available: <ul style="list-style-type: none"> • Role—Select Role and enter the complete role name. • Description—Select Description and enter the complete description of the role • Default Role—Select Default Role and enter the default role.

Step 3 Click **Add**.

The Role Management pop-up window appears.

Step 4 Enter the following details:

- Role Name—Enter the name of the role. For example, Cisco Admin.

- Description—Enter appropriate description of the role.
- Step 5** Assign appropriate tasks for the role by checking the checkbox from the Tasks tree.
You can assign specific tasks for the role by expanding and checking sub-level task nodes.
- Step 6** Click **OK** to create the role.
The role is created and is displayed in the Manage Roles page.
-

Modifying User Roles

To modify a user role:

- Step 1** Select the role you want to modify and click **Edit**.
The Role Management pop-up window appears.
You cannot change the Role Name details.
- Step 2** Modify the tasks for the role by checking or unchecking the check box from the Tasks tree.
- Step 3** Click **OK** to save the modified role.
The role is modified and is displayed in the Manage Roles pane.
-

Copying User Roles

To copy a user role:

- Step 1** Select the role you want to copy and click **Copy**.
The Role Management pop-up window appears, displaying the tasks defined for the role.
You can select or unselect the tasks by checking or unchecking the check box in the Tasks tree.
- Step 2** Enter the following details:
- Role Name—Enter the name of the role. For example, Cisco Admin.
 - Description—Enter appropriate description for the role.
- Step 3** Click **OK** to save the role.
The role is displayed in the Manage Roles pane.
-

Deleting User Roles

To delete a user role:

-
- Step 1** Select the role you want to delete and click **Delete**.
A pop-up window appears for your confirmation.
- Step 2** Click **OK** to delete the role.
The role will be deleted from the Manage Roles pane.
-

Setting Default Roles

To set a default user role:

-
- Step 1** Select the role you want to be added as a default role.
- Step 2** Click **Set as Default**.
A pop-up message appears for confirmation.
Any users added to LMS will be assigned with this role, by default.
-

Managing Users

The Manage Users task in the Getting Started flow allows you to add, edit and delete users in LMS. You can also set the authorization levels for the user.

This section explains:

- [Adding Users](#)
- [Modifying Users](#)
- [Deleting Users](#)
- [Modifying User Profile](#)

Adding Users

You can add users in LMS and associate roles for performing tasks and device level authorization.

To add a user:

-
- Step 1** Select User Management workflow from the Getting Started Assistant pane.
The following user roles and user management tasks are shown:
- Manage Roles (see [Managing Roles](#))
 - Manage Users (see [Managing Users](#))

Step 2 Click **Manage Users**.

The Manage Users page appears.

Table 9-2 describes the Manage Users page.

Table 9-2 *Manage Users Description*

Column/Buttons	Description
Username	Shows a list of users in LMS
E-mail ID	Shows the E-mail ID of the user
Add (button)	Click Add to add a user, assign roles and also provide task and device level authorization.
Edit (button)	Select a user and click Edit to modify the roles and task and device level authorization for the user.
Delete (button)	Select a user and click Delete to delete the user from LMS.
Modify My Profile	Select a user and click Modify My Profile to modify the user credentials.
Filter (button)	Click Filter . Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click Go to filter details. The following Filter By options are available: <ul style="list-style-type: none"> • Username—Select Username and enter the complete username. • E-Mail ID—Select E-Mail and enter the E-mail ID.

Step 3 Click **Add**.

The User Information pop-up window appears, displaying the fields and options for entering user information details.

Table 9-3 describes the User Information pop-up window.

Table 9-3 *User Information Field Description*

Fields/Options	Description
User Login Details	
Username	Enter a name for the user.
Password	Enter a password for the user.
Verify Password	Re-enter the password for the user.
E-mail ID	Enter the E-mail ID for the user.
Authorization Type	
Full Authorization	Select to assign full task and device level authorization for the user.
Enable Task Authorization	Select to enable task level authorization for the user and select the roles from the Roles pane.
Enable Device Authorization	Select to enable device level authorization for the user and select device groups from the Device Level Authorization pane.

Table 9-3 User Information Field Description

Fields/Options	Description
Roles	Shows the list of user roles in LMS. You can assign roles for a user by checking appropriate user roles. This list is disabled if you have selected Full Authorization as the Authorization Type.
Device Level Authorization	Shows the list of device groups in LMS. You can assign device level authorization for the user by checking appropriate device groups. This list is disabled if you have selected either Full Authorization or Enable Task Authorization as the Authorization Type.
Network Level Login Credentials	
Username	Enter the network level login username.
Password	Enter the password for the user.
Verify Password	Re-enter the password for the user.
Enable Password	Enter the enable password for the user.
Verify Password	Re-enter the enable password for the user.

Step 4 Click **OK** to add a new user.

The user is added with appropriate task and device level authorization roles and shown in the Manage Users page.

Modifying Users

You can modify the user privileges by changing the roles and the authorization levels in LMS.

To modify the user privileges:

Step 1 Select the user and click **Edit**.

The User Management pop-up window appears.

[Table 9-3](#) describes User Management pop-up window.

Step 2 Modify appropriate privileges such as roles and authorization type.

Step 3 Click **OK** to save the modified user privileges.

Deleting Users

To delete a user:

-
- Step 1** Select the user you want to delete and click **Delete**.
A pop-up window appears for your confirmation.
- Step 2** Click **OK** to delete the user.
The username gets deleted from the Manage Users page.
-

Modifying User Profile

To modify the user profile:

-
- Step 1** Click **Modify My Profile** to modify the logged in user credentials.
The My Profile window appears, displaying the following:
- User Login Details—Enter the password and E-mail credentials. E-mail address is mandatory if you assign the approver role to the local user. Otherwise, this is optional.
 - Network Device Login Credentials—Enter the network device username and password credentials.
- Step 2** Click **OK**.
-



CHAPTER 10

Managing Devices and Credentials

This chapter provides information for managing devices, configuring credential sets, applying policies, and performing device management operations.

It explains:

- [Allocating Devices](#)
- [Managing Devices using Functions](#)
- [Configuring Fallback to Secondary Credentials](#)
- [Configuring Credential Sets and Adding Devices](#)

Allocating Devices

Devices can be auto allocated to the following functions in LMS:

- Inventory, Config and Image Management
- Network Topology, Layer 2 Services and User Tracking
- Fault Management
- IPSLA Performance Management
- Device Performance Management

Devices can also be allocated based on policies that can be configured. To do this, you need to disable auto allocation all devices option and configure policies for device allocation. Auto allocation of all devices is enabled by default.

To allocate devices based on policies:

Step 1 Select Device Management workflow from the Getting Started Assistant pane.

The following Device Management tasks are shown:

- Device Allocation Settings
- Device Addition
- Policy Configuration for Device Allocation (This task appears only if you unselect **Allocate all devices** and click **Apply** in Device Allocation Settings page.)

Step 2 Click **Device Allocation Settings**.

The Device Allocation Settings page appears.

From this page, you can:

- Enable or disable auto allocation of devices for managing the functions.
- Select the device management functions that manage the allocated devices. See [Managing Devices using Functions](#) for more information.

Step 3 Unselect **Allocate all devices** check box to allocate devices based on policies. By default, **Allocate all devices** check box is selected for auto allocation.**Step 4** Click **Apply**.

The Policy Configuration for Device Allocation task appears in the Getting Started Assistant pane on the right.

Step 5 Click **Policy Configuration for Device Allocation**.

The Policy Configuration for Device Allocation page appears.

From this page, you can:

- Allocate devices by selecting device groups from the Group Selector.
- Allocate devices by creating device groups and then selecting them from the Group Selector. See *Administration of CiscoWorks LMS 4.0* for more information on creating device groups.

Step 6 Click **Apply**.

The devices in the selected groups are managed by the functions selected in LMS. See [Managing Devices using Functions](#) for more information.

**Note**

If the device selector has more than 2500 devices, it takes some time to expand the device group nodes. When the node expands, a stop script popup will appear.

If you are using IE, to view the data, click **No** from the popup window. If you are using Firefox, click **Continue**. This stop script popup will appear two or three times. Each time the popup appears, you have to click **No/Continue** depending upon your browser.

Managing Devices using Functions

You can select the following LMS functions to manage the allocated devices.

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

**Note**

If you have a 10K license, you should enable only Inventory, Config and Image Management function and disable all other functions.

To select the functions for managing the devices:

-
- Step 1** Select Device management workflow from the Getting Started Assistant pane.
- Step 2** Click **Device Allocation Settings**.
The Device Allocation Settings page appears.
Select the check box against the corresponding functions.
- Step 3** Click **Apply**.
The selected functions manage the allocated devices.
-

**Note**

If you disable a function, the function stops collecting device information, and user-defined configurations for that function will be lost. For IPSLA Performance Management, the history data will be deleted.

Configuring Fallback to Secondary Credentials

LMS uses either the primary or secondary credentials to access devices. The secondary credentials are used as a fallback when the primary credentials fail.

To enable fallback to secondary credentials:

-
- Step 1** Select Device Management workflow from the Getting Started Assistant pane.
- Step 2** Click **Device Allocation Settings**.
The Device Allocation Settings page appears.
- Step 3** Select **Fallback to Secondary Credentials** check box.
- Step 4** Click **Apply**.
-

Configuring Credential Sets and Adding Devices

You can add devices to Devices and Credential Repository (DCR) by creating credential sets and by configuring policies.

This section explains:

- [Configuring Credential Sets and Policies](#)
- [Adding Devices](#)

Configuring Credential Sets and Policies

You can create credential sets, and configure policies before adding devices to DCR. The appropriate credential set, based on the policies configured, will be used for accessing the devices.

You should configure credential sets before configuring credential set policies.

This section explains:

- [Configuring Credential Sets](#)
- [Configuring Credential Set Policies](#)

Configuring Credential Sets

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

To configure credential sets:

-
- Step 1** Select Device Management workflow from the Getting Started Assistant pane.
 - Step 2** Click **Device Addition**.
The Device Addition page appears, showing the procedure to create credential sets (See Step 1: Create Credential Sets).
 - Step 3** Click **Credential Sets**.
The Default Credential Set page appears.
 - Step 4** Click **Credential Set Name** from the Default Credentials list panel.
 - Step 5** Enter a name of the credential set in the Credential Set Name field.
The Credential Set Name can contain lower case alphabets, upper case alphabets and numerals (0 to 9).
 - Step 6** Enter a description of the credential set in the Set Description field.
 - Step 7** Select a credential type from the Default Credentials list panel and enter the respective credential information. You can select any of the credential types from the panel.
 - Standard Credentials
 - SNMP Credentials
 - HTTP Credentials
 - Auto Update Server Managed Device Credentials
 - Rx-Boot Mode Credential
 - Step 8** Enter the following credentials as required:
 - Standard Credentials
 - Primary Credentials (Username, Password, Enable Password)
 - Secondary Credentials (Username, Password, Enable Password)
 - SNMP Credentials
 - SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)

- SNMPv3 Credentials (Mode, Username, Password, Authentication Algorithm, Privacy Password, Privacy Algorithm)

You must select the SNMPv3 check box to add SNMPv3 default credentials. By default, these fields are disabled. When the SNMPv3 check box is selected, the default SNMPv3 mode is AuthPriv.

- HTTP Credentials
 - Primary Credentials (Username, Password)
 - Secondary Credentials (Username, Password)
 - Other Information (HTTP Port, HTTPS Port, Current Mode)
- Auto Update Server Managed Device Credentials (Username, Password)
- Rx-Boot Mode Credentials (Username, Password)

Re-enter the password in the respective Verify fields.

You must enter a value for at least one credential before applying the default credentials.

Step 9 Click **Apply** after you have entered all the values or click Cancel to cancel the changes.

See *Administration of CiscoWorks LAN Management Solution 4.0* for more information.

Configuring Credential Set Policies

You can configure default credential set policies and apply the default credentials for a range of devices to be added or imported to DCR.

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

To configure credential set policies:

Step 1 Select Device Management workflow from the Getting Started Assistant pane.

Step 2 Click **Device Addition**.

The Device Addition page appears, showing the procedure to configure policies for credential sets (See Step 2: Create Credential Set Policy).

Step 3 Click **Policies**.

The Default Credentials Sets Policy Configuration page appears.

Step 4 Click **Add** to add a default credential set policy.

The Add Credentials Policy Configuration dialog box appears.

Step 5 Construct a policy rule. To do so:

- a. Select a parameter from the Select a Policy Type Drop-down dialog box.

The listed parameters are IP Range, Hostname and Display Name.

Based on the parameter that you have selected, the value field name changes dynamically.

- b. Enter a value for the rule parameter.

If you have selected IP Range as the rule parameter, enter a value in the IP Range field.

If you have selected Hostname as the rule parameter, enter a value in the Hostname field.

If you have selected Display Name as the rule parameter, enter a value in the Display Name field.
The expressions in credential set policy rules are case insensitive.

- c. Select a credential set name from the Credentials Set drop-down list box to associate the rule expression with the default credential set.

Select **No Default** if you do not want to enter a credential set name.

Step 6 Click **OK** to go back to Credentials Sets Policy Configuration page.

The policy that you have configured is listed in the Credentials Sets Policy Configuration page.

You can edit a default credential set policy later. To do so, you must select a default credential set policy in the Credentials Sets Policy Configuration page and click **Edit**.

You can change the order of default credential set policy. To do so, you must select the credential set policy and use the up and down arrows to change the order.

If you want to delete a credential set policy, select the credential set policy and click **Delete**.

See *Administration of CiscoWorks LAN Management Solution 4.0* for more information.

Adding Devices

This section explains the following options to add devices into DCR:

- [Add Devices into DCR Through Discovery](#)
- [Manually Add Devices to DCR](#)
- [Import Devices into DCR](#)

The Device Addition page (Step 3: Add Devices) shows the count of the total number of devices currently in DCR.

Add Devices into DCR Through Discovery

Discovery populates only the SNMP read community string in DCR during device addition and leaves the other credentials as blank.

When other applications manage the newly added device, the management operations fail if they cannot retrieve the required credentials from DCR. To prevent the management operations failing, you can use the default credentials while adding devices through Discovery.

To add devices into DCR through Discovery:

Step 1 Select Device Management workflow from the Getting Started Assistant pane.

Step 2 Click **Device Addition**.

The Device Addition page appears, showing the option (Option 1: Configure Device Discovery) to add devices to DCR using Device Discovery.

The Discovery status shows the following information, for example:

- Discovery status: Completed
- Discovery start time: Mon Apr 12 22:54:18 IST 2010
- Discovery end time: Mon Apr 12 22:56:25 IST 2010

- Total devices discovered: 85
- Reachable devices: 37
- Unreachable devices: 48
- Devices newly added to DCR: 20
- Devices updated in DCR: 17

Step 3 Click **Edit Discovery Settings** to modify the settings to discover devices in the network.

The Module Settings page appears, where you should configure the following settings to start the Device Discovery:

- **Module Settings**—Allows you to configure or edit the Device Discovery modules to start Device Discovery
- **Seed Device Settings**—Allows you to configure or edit module-specific and global seed devices that are used to initiate Device Discovery
- **SNMP Settings**—Allows you to configure or edit the SNMP credentials required to discover the devices from the network
- **Filter Settings**—Allows you to include or exclude devices from Device Discovery and modify the filter settings. This is optional.
- **Global Settings**—Allows you to configure or modify other Device Discovery settings such as preferred DCR display name, management IP address and so on. This is optional.

See *Inventory Management with CiscoWorks LMS 4.0* for more information.

Step 4 Click **Start Discovery** to discover devices in the network.

Device Discovery starts as an immediate job. See *Inventory Management with CiscoWorks LMS 4.0* for more information.

Manually Add Devices to DCR

When you manually add devices with a similar credential set in DCR, you have to enter the credentials repeatedly for every device addition. Instead, you use the default credentials defined in default credential sets or default credential set policies to populate DCR.

To manually add devices to DCR:

Step 1 Select Device Management workflow from the Getting Started Assistant pane.

Step 2 Click **Device Addition**.

The Device Addition page appears, showing the option (Option 2: Manually Add Devices) to add devices and credentials manually to DCR.

Step 3 Click **Devices**.

The Device Properties page appears.

Step 4 Select the following management types from the drop-down list:

- Standard Type
- Auto Update Type
- Cluster Managed Type

- CNS Managed Type

You can add more than one device at a time. However, you cannot add devices of different management types.

Step 5 Enter the following device information:

- Device Type—Select the device type. For example, Cisco 10005 Router
- Display Name—Enter the display name of the device
- Host Name—Enter the host name of the device
- Domain Name—Select the domain name of the device
- IP Address—Enter the IP Address of the device

Step 6 Click **Add to List**.

The device is added to the Added Device List pane.

To remove a device from the list, select the device and click **Remove from List**.

Step 7 Select either Policy Configuration or a default credential set from the Select a Default Credential Set drop-down list, if you want to use the default credentials to access the devices.

You can select a default credential set only when you have configured at least one default credential set.

If you have opted to use the default credentials, the primary credentials, secondary credentials, Rx Boot Mode credentials, SNMP credentials, and HTTP credentials will be populated with the corresponding default values. You can click Finish to add the devices with default credentials or proceed further to make changes to the value of the credentials.

If you do not want to use the default credentials, select **No Default** in the Select a Default Credential Set drop-down list box.

Step 8 Click **Next**.

The Standard Credentials page appears.

Step 9 Enter the following credentials in the Standard Credentials page.

- Primary Credentials (Username, Password, Enable Password)
- Secondary Credentials (Username, Password, Enable Password)
- Rx Boot Mode Credentials (Username, Password)

If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.

Re-enter the value of the password in Verify field.

If you do not want to proceed further, click **Finish**.

Step 10 Click **Next**.

The SNMP Credentials page appears.

Step 11 Enter the following credentials in the SNMP Credentials page:

- SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)
- SNMPv3 Credentials (Mode, Username, Authentication Password, Authentication Algorithm, Privacy Password, Privacy Algorithm, Engine ID)

You must select the SNMPv3 check box to enter the SNMPv3 Credentials. By default, these fields are disabled. When the SNMPv3 check box is selected, the default SNMPv3 mode is AuthPriv.

Re-enter the value of Authentication Password and Privacy Password in the Verify fields.

If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.

If you do not want to proceed, click **Finish**.

Step 12 Click **Next**.

The HTTP Settings page appears.

Step 13 Enter the following credentials in the HTTP Settings dialog box.

- Primary HTTP Credentials (Username, Password)
Re-enter the value of the password in Verify field.
- Secondary HTTP Credentials (Username, Password)
Re-enter the value of the password in Verify field.
- Other Attributes (HTTP Port, HTTPS Port, Certificate Common Name, Current Mode)
Select the HTTP or HTTPS option for current connection mode.

If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.

If you do not want to proceed, click **Finish**.

Step 14 Click **Next**.

Step 15 Enter your choices for User Defined Fields.

By default, Device provides the option to define four attribute fields for a device. These fields are used to store additional user-defined data for the device.

Step 16 Click **Finish**.

A message appears that the devices are added successfully.

Step 17 Click **OK**.

The Credential Sets and Device Addition page appears.

See *Administration of CiscoWorks LAN Management Solution 4.0* for more information.

Import Devices into DCR

Importing devices from a file, NMS or any other third party applications into DCR automatically enters the SNMP read-only community string and the SNMP read/write community string.

When other functions manage the newly imported devices, the management operations fail if they cannot retrieve the required credentials from DCR. To prevent this, you can use the default credentials while importing devices from NMS or any other third party application.

To import devices into DCR:

Step 1 Select Device Management workflow from the Getting Started Assistant pane.

Step 2 Click **Device Addition**.

The Device Addition page appears, showing the option (Option 3: Bulk Import of Devices) to import devices from a file or NMS to DCR.

Step 3 Click **Devices**.

The import devices pop-up window appears, displaying the following options to import device information into DCR:

- Import From a File
- Import From Local NMS
- Import From Remote NMS

Step 4 Select the import option and update the required information.

Step 5 Select a schedule, enter the job information, and select the Default Credential Set.

Step 6 Click **Import**.

A message appears that the import job has been scheduled successfully.

See *Administration of CiscoWorks LAN Management Solution 4.0* for more information.



CHAPTER 11

Performing Advanced Configurations and Settings

This chapter guides you on performing the following advanced configurations and settings in LMS:

- Monitoring Configurations (See [Configuring Auto Monitoring](#))
- Identity Configuration (See [Configuring Identity](#))
- Fault Management (See [Managing Faults](#))
- User Role Management (See [Managing User Roles](#))
- Configuration Management (See [Managing Configurations](#))
- EnergyWise Configuration (See [Configuring EnergyWise](#))
- Collection Settings (See [Collection Settings](#))
- Group Administration (See [Administering Groups](#))

Configuring Auto Monitoring

You can configure Auto Monitoring in LMS. You can select Link Port groups or All Devices group and monitor the inter-link switches automatically. When you want to monitor these groups, pollers are created based on the polling intervals. Polling interval is 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.

Configuring Identity

Identity-based Networking Services (IBNS) is an integrated solution that comprises several Cisco products, and offers authentication, access control, and user policies to secure network resources and connectivity. With Cisco IBNS you can ensure greater security for your network and manage network changes throughout your organization in a cost-effective manner.

IBNS or Identity, as it is known in LMS 4.0, provides a set of management functions to simplify and automate the Identity management lifecycle.

Identity management in LMS 4.0 consists of:

- Identifying Identity Capable Devices, Identity Software Incapable Devices, Radius Capable Devices, and Identity Hardware Incapable Devices through a readiness report
- Preparing the network for Identity provisioning
 - Configuring RADIUS and AAA Settings
- Provisioning Identity on Identity capable devices
 - Configuring security modes, authentication profile, and host mode
 - Dynamically assigning resources
- Monitoring and reporting on user activity
- Troubleshooting authentication and authorization issues

See *Technology Work Centers in CiscoWorks LAN Management Solution 4.0* for more information.

Managing Faults

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
- 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.

Managing User Roles

After authentication, your authorization is based on the privileges that have been assigned to you. A privilege is a task or an operation defined within the application. The set of privileges assigned to you, defines your role.

The LMS authorization scheme provides you with the following system-defined roles:

- Help Desk—Can access network status information only. Can access persisted data on the system and cannot perform any action on a device or schedule a job that will reach the network.
- Approver—Can approve all tasks.
- Network Operator—Can perform all Help Desk tasks. Can perform tasks related to network data collection. Cannot perform any task that requires write access on the network.

- Network Administrator—Can perform all Network Operators tasks. Can perform tasks that result in a network configuration change.
- System Administrator—Can perform all CiscoWorks system administration tasks.
- Super Admin—Can perform all CiscoWorks operations including the administration and approval tasks. By default, this role has full privileges.

You can select a role and set it as the default role. After installing LMS 4.0, Help Desk will be the default role.

If you do not want to use the system-defined roles, you can create the custom roles and associate tasks with them.

See *Administration of CiscoWorks LAN Management Solution 4.0* for more information.

Managing Configurations

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.

The following system-defined templates are part of LMS 4.0:

- L2 Access Edge Interface Configuration
- Small Branch EIGRP DMVPN Only
- Small Branch OSPF GETVPN FaxPassThrough
- Small Branch EIGRP DMVPN FaxRelay
- Small Branch EIGRP GETVPN FaxPassThrough
- Identity - Change of Authorization

These templates are deployed using Deploy Template jobs in LMS.

See *Configuration Management with CiscoWorks LAN Management Solution 4.0* for more information.

Configuring EnergyWise

Cisco EnergyWise is a comprehensive program for power management in your network. Cisco EnergyWise enables companies to save costs by measuring, managing, and reducing the power consumption of network infrastructure, and of devices attached to the network. Cisco EnergyWise solves the problem of Network Power Management.

EnergyWise in CiscoWorks LMS 4.0 provides a set of management functions to simplify and automate the energy management lifecycle of network infrastructure, and of devices attached to the network. EnergyWise reduces the time and effort required to transform business energy policy to real energy savings.

Power management for EnergyWise in LMS 4.0 consists of:

- Grouping devices into an EnergyWise domain
- Provisioning and configuring energy policies
- Monitoring and reporting on energy consumption
- Troubleshooting power related issues

The Getting Started workflow for EnergyWise in LMS is:

- Assessing EnergyWise Readiness of your Network
- Enabling EnergyWise on Switches
- Applying EnergyWise Policies to Endpoints
- Scheduling Configuration Jobs

See *Technology Work Centers in CiscoWorks LAN Management Solution 4.0* for more information.

Collection Settings

At the time of LMS installation, system jobs are created for both Inventory collection and polling, with their own default schedules.

A periodic Inventory collection job collects inventory data from all managed devices and updates the inventory database. Similarly, the periodic polling polls devices and updates the inventory database.

You can change the default schedules of both inventory collection and polling jobs.

See *Administration of CiscoWorks LAN Management Solution 4.0* for more information.

Administering Groups

The Device Group Administration page allows you to create, manage, view, and delete device groups. The Group Selector in the Device Group Administration page contains the following predefined higher-level groups:

- System Defined Groups
- User Defined Groups

The System Defined Groups show subgroups only after the Device and Credential Repository is populated.

You can create subgroups only under User Defined Groups. You cannot create them under System Defined Groups. However, you can view the details of a subgroup under System Defined Groups and refresh the group.

Group Administration is enabled on servers in which DCR is in Master, Slave or Standalone mode. Groups created in DCR Master will be copied to Group Administration instances on servers where DCR is in Slave mode.

You can perform the following group administrative tasks:

- Creating Groups
- Viewing Group Details
- Modifying Group Details
- Refreshing Groups
- Deleting Groups
- Exporting Groups
- Importing Groups

See *Administration of CiscoWorks LAN Management Solution 4.0* for more information.



APPENDIX **A**

Troubleshooting Messages and Frequently Asked Questions in Getting Started

This appendix contains:

- [Error Messages](#)
- [Frequently Asked Questions](#)

Error Messages

This section contains the list of error messages that appear in the Getting Started workflow.

Error Message	Probable Cause	Possible Action
DCRServer is down. Check whether the process is running.	This message occurs when the DCR process or the OGSServer is not up and running.	Ensure the process is up and running.
Cisco.com credentials and E-mail settings are required to download software updates and device packages. Go to General System Settings to configure the settings.	This message occurs in the Software and Device Updates page when the Cisco.com credentials are not configured.	To configure the Cisco.com credentials, go to the General System Settings page and update the Cisco.com credentials.

Frequently Asked Questions

This section provides the frequently asked questions for Getting Started workflow in LMS:

- Q.What happens when the check box **Do not show Getting Started wizard at next login** is selected in Introduction page?
 - Q.In General System Settings page, what is the checkbox **Use of proxy for communication with Cisco.com**?
 - Q.In Multiserver Configuration page, which mode is configured by default?
 - Q.In Other System Settings page, what happens when I do not restart the daemons after changing the Browser-Server security mode?
 - Q.How to manage the devices by groups?
 - Q.How do I allocate and manage devices for the functions in LMS?
 - Q.While configuring credential sets, after entering the credential set name, the Apply button is disabled?
 - Q.What needs to be done after configuring the device discovery?
 - Q.How to create a group to allocate devices?
 - Q.Why cannot I edit or delete the default system-defined roles in LMS?
 - Q.Why am I not able to delete the logged in user?
 - Q.Why am I not able to schedule software update and device package downloads?
 - Q.Why do I get an error message as invalid argument while scheduling the schedule download for software updates or device packages?
 - Q.What happens when I select the check box **Do not show Getting Started wizard at next login** in Advanced Configurations page?
 - Q.Why the login home page is directed to dashboard while logging in as Help Desk, System Administrator, Approver or Network Approver?
 - Q.Why there is no link in Mega Menu for Getting Started when I log in as Help Desk, System Administrator, Approver or Network Approver?
 - Q.While logging into LMS, with custom role, the Getting Started workflow cannot be viewed?
 - Q.When I launch the Getting Started page, I am not able to locate the Device Management task in the Getting Started Assistant pane?
 - Q.When I launch Getting Started, the introduction page appears shrunk?
- Q.** What happens when the check box **Do not show Getting Started wizard at next login** is selected in Introduction page?
- A.** The user during the next login will be directed to the Device Status dashboard as home page.
- Q.** In General System Settings page, what is the checkbox **Use of proxy for communication with Cisco.com**?
- A.** You can select the check box and type in the Proxy server name and Port to connect to Cisco.com. You can also enter the Proxy Username and Password.
- Q.** In Multiserver Configuration page, which mode is configured by default?
- A.** By default, the CiscoWorks LMS server is in standalone with both DCR mode and SSO mode.

- Q.** In Other System Settings page, what happens when I do not restart the daemons after changing the Browser-Server security mode?
- A.** Whenever you launches the Other System Settings page, an error message is displayed on the banner mentioning `Daemons not restarted after changing the HTTPS setting`. The change will get effected only when the daemons are restarted.
- Q.** How to manage the devices by groups?
- A.** In Device Allocation Settings page, when you select the check box **Allocate all devices** and click **Apply**, the **Policy Configuration for Device Allocation** link will be shown on the workflow assistant pane on the right in Device Management.
- Q.** How do I allocate and manage devices for the functions in LMS?
- A.** Select the functions in Device Allocation Settings page for the devices to be managed and select **Allocate all devices** check box and click **Apply**.
- Q.** While configuring credential sets, after entering the credential set name, the **Apply** button is disabled?
- A.** To add new Credential Set, enter at least one credential value by selecting any one of the option below the Default Credentials.
- For Example,
- Select SNMP credential and type the RO Community String and return back to Credential set name. After entering the values in field, the **Apply** button will be enabled.
- Q.** What needs to be done after configuring the device discovery?
- A.** Once Device Discovery is configured, the **Start Discovery** button allows you to discover the device details in the repository.
- Q.** How to create a group to allocate devices?
- A.** Select **Policy Configuration for Device Allocation** from the assistant pane on the right and click **groups** (hyperlink) located above the device selector and follow the steps to create group.
- Q.** Why cannot I edit or delete the default system-defined roles in LMS?
- A.** System defined roles cannot be edited or deleted. You can edit or delete only custom user created roles. You can clone the System defined roles using the Copy option.
- Q.** Why am I not able to delete the logged in user?
- A.** You can only modify the profile of the logged in user, but cannot delete the user.
- Q.** Why am I not able to schedule software update and device package downloads?
- A.** To schedule software updates and device package downloads, you must configure E-mail and cisco.com credentials in the General System Settings page.
- Q.** Why do I get an error message as invalid argument while scheduling the schedule download for software updates or device packages?
- A.** Check if the E-mail and the Cisco.com credentials are configured in General System Settings page.
- Q.** What happens when I select the check box **Do not show Getting Started wizard at next login** in Advanced Configurations page?

- A.** The Device Status dashboard page is launched at next login. If the check box is not selected, then the Getting Started page is launched.
- Q.** Why the login home page is directed to dashboard while logging in as Help Desk, System Administrator, Approver or Network Approver?
- A.** Getting Started is not authorized for the above roles. Irrespective of the check box **Do not show Getting Started wizard at next login** selection in the Introduction page, LMS is directed to the Device Status dashboard page for the above roles.
- Q.** Why there is no link in Mega Menu for Getting Started when I log in as Help Desk, System Administrator, Approver or Network Approver?
- A.** If you are not authorized, then the menu will not have the link to launch Getting Started workflow.
- Q.** While logging into LMS, with custom role, the Getting Started workflow cannot be viewed?
- A.** If the Getting Started task is not selected, while logging you will be directed to the Device Status dashboard and the link to navigate the Getting Started workflow will not be displayed in the menu.
- Q.** When I launch the Getting Started page, I am not able to locate the Device Management task in the Getting Started Assistant pane?
- A.** Check your DCR mode in LMS. If the DCR mode is changed to slave, the Device Management task is hidden from the Getting Started Assistant pane.
- Q.** When I launch Getting Started, the introduction page appears shrunk?
- A.** If you have accessed LMS earlier and if there is an abnormal behavior in the UI, we recommend you to clear the browser cache and delete cookies before logging into LMS 4.0 again. See [Clearing Cache and Cookies](#) for more information.



INDEX

A

- Advanced Configurations [11-1](#)
 - administer groups [11-4](#)
 - collection settings [11-4](#)
 - configure auto monitoring [11-1](#)
 - configure EnergyWise [11-3](#)
 - configure identity [11-1](#)
 - manage configurations [11-3](#)
 - manage faults [11-2](#)
 - manage user roles [11-2](#)

C

- CiscoWorks LMS Interface [3-1](#)
 - adding and configuring dashboards [3-28](#)
 - adding dashboards [3-28](#)
 - copy dashboard contents [3-30](#)
 - delete dashboards [3-31](#)
 - hide dashboards [3-30](#)
 - set default dashboard [3-32](#)
 - setting dashboard types [3-28](#)
 - adding and configuring portlets [3-16](#)
 - adding CiscoWorks Product Updates portlet [3-23](#)
 - adding external links portlet [3-19](#)
 - adding frequently used links portlet [3-17](#)
 - adding IFrame portlet [3-21](#)
 - adding portlets [3-16](#)
 - adding portlets from remote server [3-19](#)
 - adding RSS portlet [3-20](#)
 - changing title of a portlet [3-25](#)
 - configuring portlets [3-24](#)
 - launching portlets [3-24](#)

- understanding portlet icons [3-23](#)
- adding links to favorites [3-35](#)
- changing portal layout [3-25](#)
- navigating legacy menu [3-35](#)
- navigating menus [3-2](#)
 - Admin [3-12](#)
 - Configuration [3-7](#)
 - Inventory [3-5](#)
 - Monitor [3-3](#)
 - My Menu [3-2](#)
 - Reports [3-10](#)
 - Work Center [3-15](#)
- understanding banner [3-1](#)
- understanding fault bar [3-34](#)
- understanding search bar [3-32](#)
 - understanding global search results page [3-33](#)
- Configuring Multiserver [5-1](#)
 - adding peer server certificate [5-6](#)
 - changing server modes to DCR [5-2](#)
 - master [5-3](#)
 - slave [5-3](#)
 - standalone [5-2](#)
 - changing server modes to SSO [5-4](#)
 - master [5-5](#)
 - slave [5-5](#)
 - standalone [5-5](#)
 - convert to master or standalone [5-2](#)
 - convert to slave [5-2](#)
 - setting up system identity account [5-6](#)
 - viewing current server settings [5-1](#)

D

- Dashboards in LMS [4-1](#)
 - Configuration [4-3](#)
 - Device Status [4-3](#)
 - EnergyWise [4-2](#)
 - Identity [4-2](#)
 - Inventory [4-2](#)
 - Monitoring [4-1](#)
 - System [4-4](#)
- Device Management [10-1](#)
 - allocating devices [10-1](#)
 - configuring credential sets and adding devices [10-3](#)
 - add devices manually [10-7](#)
 - add devices through discovery [10-6](#)
 - adding devices [10-6](#)
 - credential set policies [10-5](#)
 - credential sets [10-4](#)
 - credential sets and policies [10-4](#)
 - import devices [10-9](#)
 - configuring fallback to secondary credentials [10-3](#)
 - managing devices for functionalities [10-2](#)

G

- General System Settings [6-1](#)
 - Cisco.com [6-2](#)
 - E-mail [6-1](#)
 - Proxy [6-2](#)
- Getting Started overview [1-1](#)
 - accessing CiscoWorks Server [1-1](#)
 - getting started workflow [1-3](#)
 - logging into CiscoWorks Server [1-3](#)
- Getting started workflow [2-1](#)
 - configuring LMS [2-2](#)
 - setting getting started as the default page [2-4](#)
 - using getting started wizard [2-2](#)
 - whats new in LMS 4.0 [2-2](#)

O

- Other System settings [8-1](#)
 - Authentication [8-3](#)
 - Backup [8-2](#)
 - Browser Server Security [8-2](#)
 - RCP and SCP [8-1](#)

S

- Software, Device Package Updates and Data Migration [7-1](#)
 - procedure to migrate data [7-6](#)
 - scheduling software and device package downloads [7-5](#)
 - Software and Device Package [7-1](#)
 - Viewing packages installed [7-1](#)
 - viewing scheduled job details [7-3](#)

U

- User Management [9-1](#)
 - Managing Roles [9-1](#)
 - copying user roles [9-3](#)
 - creating user roles [9-1](#)
 - deleting user roles [9-4](#)
 - modifying user roles [9-3](#)
 - setting default roles [9-4](#)
 - Managing Users [9-4](#)
 - adding users [9-4](#)
 - deleting users [9-7](#)
 - modifying users [9-6](#)



GLOSSARY

A

AAA	Authentication, authorization, and accounting. Usually pronounced as triple-A.
AAA client	Devices added to ACS Server through which the AAA service access is attempted. The CiscoWorks Server and devices managed in CiscoWorks should be added as AAA clients in ACS.
AAA mode	Authentication Authorization and Accounting mode. By default, CiscoWorks Server authentication (CiscoWorks Local) is used to authenticate users and authorize them to access CiscoWorks applications. CiscoWorks Server can be integrated with Cisco Secure Access Control Server (ACS) to provide improved access control using authentication, authorization, and accounting.
access port	Switch port that is either connected or not connected to a Layer 2 device, or is connected to a non-Layer 2 device (such as a router). In LMS, this is a switch port that is connected to an End host or IP Phone.
acknowledging discrepancy	Removing a discrepancy from the Unacknowledged Discrepancies report.
acknowledging discrepancy	Process that discovers End Hosts and IP Phones connected in the network.
Associated ACL	This ACL allows selective access control to introduce a higher level of access security for low impact mode and high security mode.
Active Directory	Microsoft Active Directory. A pluggable authentication module that provides AAA services to CiscoWorks Server when integrated.
Active end host	End hosts that are currently connected to the network.
Active state	In LMS, Active state indicates that LMS is currently polling for the device MIB instance.
Active switch	After converting two VSS-enabled Standalone switches into a Virtual Switching System, one switch becomes the Active switch and other the Standby switch.
activity trace	Lists activity on the server running CiscoView (for example, launching the Ethernet Statistics dialog box).

adapter	Program that links a domain manager to its environment. Adapters forward inventory and event information to a domain manager for analysis. These adapters send the results of the analysis to other network management applications or other adapters.
Add devices	Sub-step in the Server Set up workflow. LMS allows you to add devices using multiple methods, simultaneously. You can add devices using the Import from File or NMS feature, and Campus Device Discovery.
Address Resolution Protocol	See ARP .
Adhoc Devices	Cisco devices or devices with a unique IP address.
Adhoc Target Device	External target devices that are added to LMS.
aggregate device	Device that contains more than one intelligent management agent, each with its own IP address. CiscoWorks recognizes such devices as multiple devices. For example, an MSFC on a switch. Also called a Containing or Composite device.
AIX	Advanced Interactive Executive: IBM's version of Unix.
alert	Indicator that is generated in LMS that indicates an abnormal condition in the network. An alert consists of related events. A finite set of alerts are displayed on the Alerts and Activities display.
Alias devices	Devices in LMS with different hostnames or IP addresses. When a new device is added to LMS, it may already exist in LMS, with another hostname or IP address. This device will be in the Alias state.
Allocate devices	Sub-step in the Getting Started workflow. This helps you to allocate devices that are managed by the functions in LMS.
ANIServer	Process that performs Data Collection. See also Data Collection .
Apache	Web server used in CiscoWorks Server on both UNIX and Windows systems. This hosts the base CiscoWorks Home Page and all major applications.
API	Application Programming Interface. A language and message format used by an application to communicate with the operating system and other services, such as a database management system or communications protocol.
Application Programming Interface	See API .
Application Registration	<ol style="list-style-type: none">1. Process of registering the CiscoWorks applications with CiscoWorks Home Page on the local or remote servers.2. Process of moving the information from CiscoWorks Server to ACS Server. Only when the applications are registered, can CiscoWorks use the AAA services from the integrated ACS server for user authentication and authorization.

Application Service Adapter	See ASA .
Application specific groups	Groups based on device types or states specific to CiscoWorks applications. The application-specific groups appear in the device selector of the respective applications.
Application view	Views that are displayed in CiscoWorks LMS Portal. These views are based on the installed applications. For instance, CS View (Common Services View).
Approver	Predefined role in CiscoWorks applications. Users assigned with this role can approve all CiscoWorks tasks.
Archive Management	Maintains an active archive of the configuration of devices managed by LMS. It enables you to fetch, archive, and deploy device configurations. It also lets you search and generate reports on archived data, compare and label configurations, compare configurations with a baseline, and check for compliance.
archived report	A report is archived when a scheduled report job is completed successfully.
ARP	One of the Discovery protocols supported by LMS Device Discovery. This Discovery module depends on the Routing Table Discovery module.
AS	Single Sign-On Master server providing authentication services to other CiscoWorks Server configured in the same domain.
ASA	Application-specific information repository. It is a source of devices and attributes that are grouped by the Groups server. It is also an interface among applications and the Groups server.
ASCII	American Standard Code for Information Interchange. 8-bit code for character representation.
Assertion error	Sybase Assertion error that occurs when the LMS databases do not run. This error appears if any anti-virus software or third-party backup software is used in the CiscoWorks Server.
Audit Trail	It tracks and reports changes that the administrator makes on the LMS server.
AUS	Web-based interface to upgrade device configuration files and software images on firewalls that use the Auto-update feature. You can use this interface to add, edit, and delete devices.
Auth password	SNMPv3 authentication password used to operate the devices in AuthNoPriv and AuthPriv modes.
Auth protocol	SNMPv3 authentication algorithm used in AuthNoPriv and AuthPriv modes. The authentication algorithm can be MD5 or SHA-1. These protocols ensure message integrity and protection against message replays.

Authentication mode	Mode selected to authenticate the CiscoWorks users when logging into the CiscoWorks Server. Either the ACS server or the CiscoWorks Server can provide the authentication services, based on the AAA mode set up in CiscoWorks.
Authentication Profile	Authentication profile selects the method of authentication to be used. Multi-method profiles provide a fallback order, if the first method fails, the second method will take over.
AuthNoPriv	One of the security levels within SNMPv3 providing message integrity and authentication security features.
Authorization mode	Mode selected to authorize the user after authentication. The Authorization services can be provided by the ACS or by the CiscoWorks Server.
AuthPriv	One of the security levels within SNMPv3 providing message integrity, authentication, and data encryption features.
Auto mode	Mode in which devices are managed in LMS. In this mode, all devices in DCR are automatically managed in LMS. Filter policies can be set to manage certain devices/set of devices.
Automonitoring	Monitors the inter-link switches automatically.
Auto Smartports	Auto Smartports macros dynamically configure ports based on the device type detected on the port. When the switch detects a new device on a port it applies the appropriate Auto Smartports macro to the port.
Auto Smartport macros	<p>Allows you to save and share common configurations. Each Smartport macro is a group of CLI commands. When you apply a Smartport macro on a port, the CLI commands within the macro will be deployed on the port.</p> <p>If the command fails when applying a macro, either because of a syntax error or a configuration error, the macro continues to apply the remaining commands on the port. As part of provisioning Smartport, LMS provides the following Netconfig tasks:</p> <p>Auto Smartports—Task applicable for Device based Netconfig flow. See also Auto Smartports.</p> <p>Manage Auto Smartports—Task applicable for Port based Netconfig flow. See also manage Auto Smartports.</p> <p>Smartports—Task applicable for Port based Netconfig flow. See also Smartports.</p>
Auto Update server	See AUS .
Availability	Checks the reachability of the target device, based on the successful completion of the RTT operation from source to target. The availability is reported as a percentage.

B

Backup data	See database backup .
bandwidth utilization	Measure of traffic flowing across a link.
Baseline template	<p>You can identify a set of standardized policy-based commands that you want to have on a set of devices.</p> <p>You can create a Baseline template (a set of commands identified through baselining) that contain placeholders for device-specific values to be substituted.</p>
Best Practice Deviation	Best practices that are recommended by Cisco but not implemented in the network.
BGP	<p>One of the discovery protocols supported by LMS Device Discovery.</p> <p>This discovery module uses Border Gateway Peer Table to identify its BGP peer.</p>
BIRT	Business Intelligence and Reporting tool.
Border Gateway Protocol	See BGP .
broker	LMS software that communicates between a domain manager and its clients.
Browser server security	<p>Security feature that LMS provides for secure access between the client browser and the management server.</p> <p>LMS uses SSL to provide browser server security.</p>
Bug Toolkit	Application in LMS that helps you identify the bugs filed against devices in their network. It also helps you to check the status of the bugs.
Built-in Group	In a Smart Install network, these groups are used to configure homogenous groups.

C

CA	<p>Authority in a network that issues and manages security credentials and public keys for message encryption.</p> <p>As part of a public key infrastructure, a certificate authority checks with a registration authority to verify information provided by the requestor about a digital certificate. If the registration authority verifies the requestor's information, the certificate authority issues a certificate.</p>
called number	Destination telephone number of the call.
calling number	Telephone number from which the call originated.

Catalyst Integrated Security features	<p>You can use the Catalyst Integrated Security Features task to configure Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard and Security Violation on ports.</p> <p>The Catalyst Integrated Security Feature is supported only on Catalyst 2960, 3560, 3560E, 3750, 3750E switches.</p> <p>This task is available only in the Port based flow of a NetConfig job.</p>
category	Command or option specific to a selected device in CiscoView. You can modify or view categories to configure and monitor a device, card, or port.
CCO	Cisco Connection Online (former name of Cisco.com). The name of Cisco Systems' external web site.
CCR	CiscoWorks component that manages the seamless installation, upgrade, patching and uninstallation of Multiple Device Controller modules, and the Core module.
CDP	<p>Media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. It runs on all media that support SNAP, including LANs, Frame Relay, and ATM media.</p> <p>Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN.</p>
certificate	See security certificate .
Certificate Authority	See CA .
CFM	Connectivity Fault Management.
Change Audit	<p>Tracks and reports changes made in the network. Change Audit logs information changes to a central repository.</p> <p>Device Configuration, Inventory, and Software Management changes can be logged and viewed using Change Audit.</p>
Change Audit reports	<p>Contains all change information provided by LMS, based on filter criteria. You can generate a Change Audit report for selected devices.</p> <p>It displays all changes that have been logged for the devices. The types of Change Audit reports are, 24-hour report, Exception period report, and Standard report.</p>
Change of Authorization (CoA)	CoA provides a mechanism for changing the attributes of a session after it has been authenticated.
Channel Interface Processor	See CIP .

chassis view	Browser page that displays a graphical representation of a device's front or back panel after you select a device in CiscoView. Device components are color-coded according to their status and refreshed according to the polling frequency you have defined.
Child group	Groups and sub-groups that are part of container group.
CIP	Channel attachment interface for Cisco 7000 series routers. The CIP connects a host mainframe to a control unit, eliminating the need for an FEP for channel attachment.
Cisco Discovery Protocol	See CDP .
Cisco IOS software	<p>Cisco Internetwork Operating System software. Cisco system software provides common functionality, scalability, and security for many Cisco products.</p> <p>The Cisco IOS software allows centralized, integrated, and automated installation and management of internetworks. It supports a wide variety of protocols, media, services, and platforms.</p>
Cisco TAC	Cisco Technical Assistance Center. There are four TACs worldwide.
Cisco.com Fetch Interval	<p>LMS allows you to configure the interval at which PSIRT and End of Sale or End of Life information is retrieved from Cisco.com.</p> <p>The information retrieved is stored in the database. This database is queried to generate PSIRT Summary report or the End of Sale and End of Life reports.</p>
CiscoView Planner page	Page from which you can download the latest CiscoView device packages.
CiscoWorks Command Line Interface	See cveli .
CiscoWorks Home Page	Default home page that appears if you log into a CiscoWorks Server. If you have installed LMS Portal on the same CiscoWorks Server, LMS Portal will be the default home page.
CiscoWorks Local mode	One of the AAA modes. In the CiscoWorks local mode, authentication and authorization services are provided by the local server. Also known as Non-ACS mode.
CLI	Interface that allows you to interact with the operating system by entering commands and optional arguments. The Solaris operating system and DOS provide CLIs.
Cluster Discovery Module	<p>One of the discovery protocols supported by LMS Device Discovery.</p> <p>This module discovers the devices in a DSBU cluster and queries the Cluster MIB to discover all members of the cluster.</p>
Cluster managed device	One of the device management types in DCR Administration. The Cisco clusters and their member devices are managed using this device management type.

Cluster Switches	A group of switches connected to each other, where one switch is designated as the Command switch and upto 15 switches can be designated as Member switches.
CN	Certificate Common Name.
CNS managed devices	One of the device management types in DCR Administration. Refers to the devices managed by Cisco Networking Services.
collector	Entity that encompasses a source router, a target device, an operation, and collector schedule details.
collector groups	Allows you to associate a group of collectors. The collector groups are defined based on a set of criteria such as operation name, operation type, source address, target address.
collector schedule duration	Indicates for how long (in days, hours, and minutes) the collector runs and gathers information from the source router. The default Start Time for a Collector is Immediate. The default End Time for a Collector is Forever. The polling period is set from 00:00:00 hours to 23:59:59 hours on a daily basis.
Command Line Interface	See CLI .
Command sets	Represents a logical grouping of commands. Each command set is associated with a unique name.
Comma Separated Values	See CSV .
Common Name	See CN .
Common Object Request Broker Architecture	See CORBA .
community string	Text string that acts as a password and authenticates messages sent between a management station and a router containing an SNMP agent. The community string is sent in every packet between the manager and the agent. Also called a community name.
Compliance Management	Option in LMS Configuration Management which deals with creating, maintaining and comparing Baseline Templates. You can create a baseline template and compare it with the configurations available on devices to check compliance.
composite device	See aggregate device .
Config Editor	Option in LMS that provides easy access to configuration files. Config Editor allows a network administrator with the appropriate security privileges to edit a configuration file that exists in the configuration archive.

Configuration Dashboard	Configuration Dashboard in LMS provides information such as, date of last configuration change, status of the configuration jobs, summary of inventory configuration protocol, Hardware and Software summary.
Configuration Management	Stores the current, and a user-specified number of previous versions, of the configuration files for all supported Cisco devices maintained in the LMS. It tracks changes to configuration files and updates the database if there are any changes.
Configure Range	Tab on the Run Discovery on server page (Add Devices) allows you to limit discovery by IP addresses in your network. Establishing IP address boundaries prevents discovery from occurring outside these boundaries.
conflicting device	Device that is both in the import source and in DCR but differs in its attributes. The DCR Import Status report displays the conflicting devices after every Import operation.
Connectivity Group	This is a custom group which is used to set up the image and configuration file for all client switches that match connectivity.
Connectivity status	Table in LMS that provides information on device connectivity. It displays the Ping, Trace route, Telnet statuses of the device, along with other related information.
contained device	Subordinate device that resides inside an aggregate (or containing) device. For example, an MSFC in a switch).
container group	Groups without a rule. The group membership is the union of the membership of its subgroups. If a container group does not have subgroups, the membership list will be blank.
containing device	See aggregate device .
context menu	Menu that appears when you right-click a device or its components in CiscoView. The items in this menu are context-sensitive and vary according to the device and your selection.
Contract Connections	<p>Application allows you to see the status of service contracts of all IOS devices in the network. Contract Connection allows you to verify which of your Cisco IOS devices are covered by a service contract.</p> <p>Contract Connection (CC) uses Inventory Manager, Cisco.com, and Cisco's internal contract tracking service, Contract Agent, to provide the status of the service coverage. You can generate Contract Connection reports using Reports Center.</p>
COS	Class of Service.

CORBA	<p>Industry standard middleware architecture developed and maintained by the Object Management Group.</p> <p>CORBA services act as communication mechanisms to develop distributed applications. CORBA is platform and language neutral. This means that a C application running on a PC can communicate with a Java application running on Solaris.</p>
Core Client Registry	See CCR .
core file	<p>File created by the Operating System in CiscoWorks Server when a program is abnormally terminated.</p> <p>The core file is created in the <i>NMSROOT\bin</i> directory on CiscoWorks Server and stores important data about processes.</p>
Critical Device Poller	Polls only a critical set of devices in the network. You can use this option to see the device and link status without running Data Collection.
CS	Represents a common set of management services that are shared by CiscoWorks applications. This provides a foundation for CiscoWorks applications to share a common model for data storage, login, user role definitions, access privileges, security protocols, as well as navigation.
CSR	Certificate Signing Request file.
CSV	Interchange file format used to export and import spreadsheets or other tables. Each line in the ASCII file represents a row of data from a table. Each line contains the data elements from a row of the table, with individual table values separated by comma characters.
custom layout	Special layout of report columns to suit specific needs. The layout can be designed by selecting and arranging the required columns from the available ones.
custom report	Report with a customized layout to suit specific needs.
Custom Report feature	CiscoWorks LMS allows you to create reports using MIB variables that are either common to all Pollers or specific to a Poller polled by LMS. These reports are called Custom Reports.
Custom Report Template	Option available under Reports that allows you to create new report templates, customized according to their requirements. You can edit, or delete existing custom templates.
Customer Edge Router	Router on the border between a VPN provider and a VPN customer that belongs to the customer
cwcli	A netshow command that let you use NetShow features from the command line. You can use the cwcli netshow commands to view, browse, create, delete, and cancel NetShow jobs and Command Sets.

cwcli config	CiscoWorks configuration command-line tool of LMS. It allows you to update devices and archive configurations, delete configurations and compare configurations.
cwcli export	CiscoWorks export command-line tool of LMS. This command-line tool provides servlet access to Inventory, Configuration and Change Audit data.
cwcli inventory	CiscoWorks Device Management application command-line tool of LMS. You can use this tool to check the device credentials, export the device credentials, view or delete the LMS devices.
cwcli invreport	CiscoWorks Inventory command-line tool of LMS. It allows you to run previously created Inventory Custom reports and also system reports. The output is displayed in the (CSV) Comma Separated Value format.
cwcli netconfig	CiscoWorks netconfig command-line tool of LMS. It allows you to use NetConfig from the command line.
cwcli netshow	CiscoWorks NetworkShow (NetShow) command-line tool that enables users to use NetShow features from the command line. You can use the cwcli netshow tool to view, browse, create, delete, and cancel NetShow jobs and Command Sets.

D

Daemon Manager	Daemon is a long-running background process that answers requests for services. Daemon Manager controls the various daemons running and can be used to start, stop, or monitor them.
Dashboard	<p>Dashboards provide you with a quick snapshot of specific functions in LMS. The following functional dashboards are available in LMS:</p> <ul style="list-style-type: none"> • Monitoring Dashboard • Identity Dashboard • EnergyWise Dashboard • Inventory Dashboard • Configuration Dashboard • Device Status Dashboard • System Dashboard
Data Collection	Fetches the device list from DCR and collects complete information about the devices.
Data Collection filters	Filters that you can set to either include or exclude of IP address ranges in Data Collection.
Data Extraction Engine	Utility to export LMS data in XML format.

data trace	Specifies standard network traffic trace between IP addresses or named devices.
database backup	Saving the database to maintain a safe copy of data. To start backing up data, you must have enough storage space on the target location.
database restore	Restoring the data that you had backed up earlier on the CiscoWorks Server.
data-link switching	See DLSw .
DCR	Common repository of devices, their attributes, and credentials that are used by various network management applications.
DCR Administration	Interface to administer the common repository of devices, their attributes, and credentials used by CiscoWorks applications.
DCR Master	Hosts the authoritative, or a master-list of all devices and their credentials. All other DCRs in the same management domain that are running in the Slave mode, normally share this list.
DCR modes	<p>DCR works based on a Master-Slave model. The Master hosts the authoritative, or a master-list of all devices and their credentials. All other DCRs in the same management domain that are running in the Slave mode, normally share this list.</p> <p>DCR can also be in the Standalone mode. In the Standalone mode, DCR maintains an independent repository of device list and credential data. See also DCR.</p>
DCRDevicePoll	LMS backend process that initiates device polling. It uses SNMP and ICMP protocols to check whether the devices are reachable.
DCR Slave	DCR mode that runs as a Slave to a Master server in the same management domain and shares the device list from the Master.
DCR Standalone	DCR mode that maintains an independent repository of the device list and the credential data.
dcrccli	Utility provided with CiscoWorks to perform the device management tasks through CLI.
debugging	Finding reasons for runtime issues. Enabling debugging options creates log files. You can use these log files to find the cause for a runtime problem.
default credentials	<p>Default credentials are stored in DCR and are not associated with any device. You can use them to add or import a set of devices in DCR with common credentials.</p> <p>See also default credential set.</p>
default credential set	<p>Credential set that comprises Primary credentials, Secondary credentials, SNMP credentials, HTTP credentials, AUS managed credentials, and Rx-Boot mode credentials.</p> <p>You can configure multiple default credential sets. You can set these default credential sets for a range of devices to be added or imported to DCR based on certain policies.</p>

Delete interval	Time interval at which records from End host table, IP Phone table, Wireless end hosts table, and the History table are deleted.
Desktop Switching Business Unit	See DSBU .
Detailed Device report	<p>One of the Inventory reports. It displays detailed hardware, software characteristics and physical containment information for one or more selected devices.</p> <p>The hardware and software characteristics include System, Port Interface, Bridge, Memory Pool, Flash Devices, and Image. The physical containment information includes Stack, Chassis, Module, and Processor information.</p>
Device Allocation Policy	The policy you must configure to manage the devices in your network.
Device and Credential Repository	See DCR .
device attributes	Unique identifiers of a device such as domain name, hostname, device identity and management IP Address.
device based acquisition	Process that discovers the End Hosts on all the VLANs in the selected device. Helps you to collect information only on End Hosts connected to the specified device.
Device Based VRF report	Displays the VRF details specific to the VRF configured devices selected while generating the report. See also VRF-Lite .
Device Center	Provides a device-centric view for CiscoWorks applications and device-oriented navigation paradigm. This provides device-centric features and information from a single location.
Device Credentials	Values that are used by applications to access and operate on devices. It is typically an SNMP community string or a user ID and password pair.
Device Diagnostic Tools	Portlet from where you can launch Device Troubleshooting workflow and Device Center. See also Device Troubleshooting .
Device Discovery	Discovers the devices available in the network, starting from the seed device and updates the information to DCR. See also seed device .
Device Management	<p>Device Management refers to adding, editing and deleting devices in LMS. In other words, it refers to managing devices in LMS.</p> <p>In addition to these tasks, Device Management also verifies the device credentials. Device Management also consists of Inventory Management and Group Administration.</p>
Device Management mode	Mode in which the devices are managed in CiscoWorks application. It can be either Auto mode or Manual mode.

Device Map	List of all supported devices on a CiscoWorks Server maintained by Software Center.
Device package	Software update that enables CiscoView to support new features for a particular device.
Device Package Updates	<p>Applications that provide support for a range of devices by installing device packages.</p> <p>You can add device packages to the applications anytime after the initial product release or installation. When new device packages become available, they are placed on Cisco.com.</p>
Device Poller	Process that polls the devices in the network. Polling checks if the devices managed by LMS are SNMP reachable, and if the interfaces in the devices are up or down.
Device report	<p>In LMS, this report displays all performance parameters of a device, such as memory utilization, CPU utilization, interface utilization, environmental temperature, Poller failures and so on.</p> <p>The Device report also displays the polled data for MIB variables added in the user-defined templates.</p> <p>LMS generates Device report based only on the data for the last 24 hours.</p>
Device Selector	Device Selector allows you to search the devices in DCR. It helps to locate the devices and quickly perform the various device management tasks.
device state	Management state of a device. Can also pertain to the device discovery state. See also management state and Discovery state device.
Device Troubleshooting	<p>One of the LMS workflows. Device Troubleshooting workflow helps you identify why a device is unreachable.</p> <p>The generated Device Troubleshooting report contains details on device topology, network inconsistencies, misconfiguration, and Alerts and Syslog Messages for the selected device.</p>
DfmServer/DfmServer 1	<p>Infrastructure device domain manager, a program that provides backend services for Fault Management. Services include SNMP data retrieval and event analysis. The DfmServer log is NMSROOT/objects/smarts/log s/DFM.log.</p> <p>If there are two instances of the DfmServer running, each will have a log file, DFM.log and DFM1.log.</p>
DHCP	Dynamic Host Configuration Protocol. Allows you to allocate IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DiscoveryCli	A command line utility used to start, stop and view the current status of Device Discovery.
Discovery, device	In LMS, this is the process of probing to analyze a network element. Also referred to as collection.

Discovery Filters	Allows Device Discovery to exclude or include devices from the network, based on some rules.
Discovery Modules	Various protocols used by Device Discovery to discover the devices from a network.
Discovery state	Condition that a device passes through while being probed. After Discovery, the device information is added to the inventory. Device Discovery states include Known, Learning, Questioned, Pending and Unknown.
discrepancy	Network inconsistencies or anomalies or misconfigurations in the discovered network. They have a severe impact on the network connectivity.
Diskwatcher	Back-end process that monitors disk space availability on the CiscoWorks Server. This process calculates the disk space information of a drive (on Windows) or a file system (on Solaris) where CiscoWorks applications, are installed and stores them in diskWatcher.log file.
Distinguished Name	See DN .
DLSw	Data-link switching. Interoperability standard, described in RFC 1434, allows you to forward SNA and NetBIOS traffic over TCP/IP networks using data-link layer-switching and encapsulation. DLSw uses SSP instead of SRB, eliminating the timeouts, lack of flow control, and lack of prioritization schemes. See also SRB and SSP .
DN	Unique name used by authentication servers when you integrate CiscoWorks Server with external MS Active Directory or IBM SecureWay Directory servers. Distinguished Name is usually composed of the three parts: prefix, usersroot and login.
DNS	Domain Name System. System used in the Internet for translating names of network nodes into addresses.
Domain manager	See DfmServer/Df mServer 1 .
Domain Name System	See DNS .
domain server	See Domain manager .
Dormant MAC	MAC Addresses that are inactive for the specified number of days.
DSBU	Desktop Switching Business Unit. One of the business units of Cisco.
DSBU cluster	See Cluster managed device .
duration	Number of minutes that a collector actively collects network performance statistics at the source router. The default value is Forever.
dynamic group	Group for which the membership list is automatically recomputed whenever it is invoked and is always current.

Dynamic Host Configuration Protocol	See DHCP .
Dynamic Updates	Same as Dynamic User Tracking .
Dynamic User Tracking	Asynchronous updates based on SNMP MAC notifications traps. These updates are used by LMS to track real time changes in the end hosts connected to the network.

E

Echo	Measures the total round-trip latency and other statistics and errors from the source router to the target device.
EDS	Event management software that allows you to send messages from one process to another in a networked and distributed environment.
EEM	Embedded Event Manager is an IOS technology that runs on the control plane of the Cisco Catalyst 6500 device. This EEM technology is integrated within Cisco IOS Software and because of this, the Cisco IOS Software EEM is aware of the state of the network from the perspective of view of the device on which it is operating.
Embedded Event Manager	See EEM .
End Host/IP Phone Down	One of the LMS workflows. The generated End Hosts/IP Phone Down report helps you locate and track the End Hosts/IP Phone in your network. They also provide information to troubleshoot and analyze the connectivity issues.
End of Sale/End of Life report	See EoS/EoL report .
End of Sale/End of Life Hardware report	<p>Inventory report that is generated based on the End of Sale/End of Life information retrieved from Cisco.com at regular intervals.</p> <p>This report helps you to ascertain the end-of-sales and end-of-life information for devices and modules in the network. It provides a summary of the end-of-sale or end-of-life alerts based on the selected devices.</p>
End of Sale/End of Life Software report	<p>Reports that provide information on the end-of-sale, end-of-life, and the end-of-engineering dates for the software image versions running on the devices in your network.</p> <p>You can generate an EoS/EoL Software report for software images based on the information retrieved from Cisco.com at regular intervals.</p>
EnergyWise	<p>EnergyWise is a comprehensive program for power management in your network.</p> <p>EnergyWise in CiscoWorks LMS 4.0 provides a set of management functionalities to simplify and automate the energy management lifecycle of network infrastructure, and of devices attached to the network.</p>

EnergyWise Domain	An EnergyWise domain consists of Cisco domain members and end points. A domain can represent a geographic location, a specific place in the network, or any energy specific logical representation.
EnergyWise Endpoint Groups	You can create endpoint groups to group endpoints based on certain filters like role, importance, and keywords. The endpoints can be part of one or more domains. After you create an endpoint group, you can apply policies to the group.
EnergyWise Policies	You can configure EnergyWise policies, a set of recurring events, to manage the power usage of devices in the network.
EoS/EoL report	See End of Sale/End of Life Hardware report and End of Sale/End of Life Software report .
Error device	Device that is not successfully added or imported to DCR. The error devices are listed in DCR Device Addition Summary or DCR Import Status report after the Add or Import operation.
ESS	Asynchronous messaging service that provides a messaging infrastructure based on a publish-and-subscribe paradigm. It enables distributed, loosely coupled interprocess communications.
ethernetJitter	Ethernet Jitter is an IPSLA Operation. LMS provides the option to create, modify, or delete your own Ethernet Jitter operations from the List of Operations page for measuring performance between a source and MEP.
ethernetJitterAutoIPSLA	Ethernet Jitter Auto IPSLA is an Auto IPSLA Operation. LMS allows you to create, modify, or delete your own Ethernet Jitter Auto IPSLA operations from the List of Operations page for measuring performance between a source and MEP.
ethernetPing	Ethernet Ping is an IPSLA Operation. LMS allows you to create, modify, or delete your own Ethernet Ping operations from the List of Operations page for measuring Round-trip time latency and Errors between a source and MEP.
ethernetPingAutoIPSLA	Ethernet Ping Auto IPSLA is an Auto IPSLA Operation. LMS allows you to create, modify, or delete your own Ethernet Ping Auto IPSLA operations from the List of Operations page for measuring performance between a source and MEP
event	Indicator that is generated in LMS when a fault occurs on a network. Related events are “rolled up” into alerts. A finite set of events is displayed on the Alerts and Activities Detail page.
Event Distribution System	See EDS .
Event Forensics	Event Forensics refer to additional information related to the specific events that are polled by LMS server.

Event Monitor	A centralized place where in you can view the event details of all devices.
Event Services Software	See ESS .
Extensible Markup Language	See XML .
Extensible Stylesheet Language	See XSL .

F

fallback option	Allows you to access the software if the login module fails, or if you accidentally lock yourself or others out. The fallback options are available only for non-ACS login modules.
FAT	A file system table used by the FAT file systems.
Fault Monitor	A centralized browser where you can view the information on faults and events of devices in a single place.
File Allocation Table	See FAT .
File Transfer Protocol	See FTP .
firewall	One or more routers or access servers designated as a buffer between any connected public networks and a private network to ensure security.
FPM	<p>Flexible Packet Matching (FPM) is a next-generation Access Control List (ACL) technology that is capable of filtering IP packets at a bit-level. As part of provisioning, LMS provides the following netconfig tasks that allow you to configure FPM in the devices:</p> <ul style="list-style-type: none">• FPM Package Group—Task applicable for Device based Netconfig flow• FPM Package-Info—Task applicable for Device based Netconfig flow• FPM Policy—Task applicable for Port based Netconfig flow
FPM Package Group	<p>You can use the FPM Package-Group task to add, edit and remove FPM package groups.</p> <p>The FPM Package-Group task is available only in the Device based flow of a NetConfig job.</p>
FPM Package-Info	<p>You can use the FPM Package-Info task to configure FPM package info on the devices.</p> <p>The FPM Package-Info task is available only in the Device based flow of a NetConfig job.</p>

FPM Policy	<p>You can use the FPM Policy task to attach or detach package groups to or from an interface.</p> <p>The FPM Policy task is available only in the Port based flow of a NetConfig job</p>
FQDN	Fully Qualified Domain Name consisting a host name and domain name.
Frequently Used Links portlet	Helps you to view the frequently used links. You can also add, modify and remove the frequently accessed links.
FTP	File Transfer Protocol (FTP) operation allows you to measure the network response time between a Cisco device and an FTP server to retrieve a file.
Functional View	Default view when you log into CiscoWorks for the first time. For subsequent logins, you can set any view as the default view. Contains portlets that help you to launch the applications installed in the CiscoWorks Server.

G

Generic OnLine Diagnostics	See GOLD .
Getting Started workflow	<p>Getting Started workflow in LMS assists you in performing the following basic tasks required to get your CiscoWorks LMS running:</p> <ul style="list-style-type: none">• Understanding the Procedure to Migrate Data• Configuring E-mail, Cisco.com and Proxy Settings• Configuring Multiserver Setup• Checking Protocol, Security, Backup and Authentication Settings• Managing Devices and Credentials• Managing User Roles and Users in LMS• Updating Software and Device Packages• Advanced Configurations and Settings <p>You can configure these tasks step-by-step or configure them separately at different intervals. You can select the task using the Getting Started assistant pane.</p>
Global seed devices	Seed devices that are common to all Discovery modules selected for a Device Discovery process.
GOLD	Device-specific IOS feature with fault detection capabilities. It defines a common framework for diagnostic operations across Cisco platforms running Cisco IOS Software.

GOLD Health Monitoring Task	<p>Task that allows you to configure GOLD Health Monitoring tests on Cisco Catalyst 6500 IOS switches device categories.</p> <p>This task is available only for the Module-based netconfig job wizard. See also GOLD.</p>
Graphical User Interface	See GUI .
group	Named aggregate entity comprising a set of devices belonging to a single class or a set of classes, with a common superclass. Groups can be shared among users or applications, subject to access-control restrictions. The membership of a group is determined by a rule.
Group Admin	Allows you to interact with the Groups Server to create and manipulate groups using Group Admin.
Group Hierarchy	Hierarchical fashion of groups and subgroups.
Group Membership	Allows you to assign objects to a group or exclude objects from a group.
Group Rule	Consists of one or more rule expressions combined by operators. These operators can be AND, OR or EXCLUDE. A rule always evaluates to objects of a particular class defined in an application schema.
Group Selector	List-tree that displays all device groups. Allows you to add a device to the tree and modify, view or refresh the group details. You can also add the groups to the group selector or remove them from the list-tree.
Group Server	Manages groups of devices. It helps you to create, edit, delete, and refresh groups to be shared by the application. It interfaces with an application service adapter to evaluate group rules and retrieve devices of a particular group.
GUI	<p>User environment with textual and graphical representation of the application.</p> <p>Conventions such as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are examples of platforms using a GUI.</p>

H

Help Desk	Predefined role in CiscoWorks. Users with this role can access network status information only. Can access persisted data on the system and cannot perform any action on a device or schedule a job that will reach the network.
Hewlett Packard OpenView	See HPOV .
Hierarchical maps	Topology views that display the devices listed under Topology Groups in a hierarchical way. Each map displays the selected group as a cloud of devices. If there are parent and sub-groups, the sub-group is displayed inside the corresponding parent group as a cloud icon.

High Security Mode	High Security Mode ensures the highest security level of LAN-based access, where access is not granted unless authentication succeeds.
Histo Graph-It	Portlet that enables you to query the information of a particular MIB variable in a device for a specified period of time and generate a graph.
Historical reports and graphs	LMS generates these reports and graphs that contain statistical data for a single or group of collectors based on the granularity, such as hourly, daily, monthly, or weekly.
History report	Tracks the log in and log out information about the End Hosts and the users in your network.
hop	Passage of a data packet between two network nodes. For example, between two routers. See also hop count .
hop count	Number of hops till which the network topology is drawn in N-Hop view portlet. See also hop .
host	Computer system on a network. Similar to the term node, except that host usually implies a computer system, whereas node generally applies to any network system, including access servers and routers.
Host Mode	Host mode determines the number of hosts that can be authenticated on a given port.
Hostname change script	CLI utility to update the new hostname information in the CiscoWorks directories and files, registry entries, and databases. This occurs after you have changed your hostname in the CiscoWorks machine.
Hot Standby Router Protocol	See HSRP .
HPOV	Hewlett Packard OpenView. A third party software used as network management systems for CiscoWorks Applications.
HSRP	One of the Discovery protocols supported by Device Discovery. This module discovers the devices from the HSRP group which consists of an active router and Standby routers. If the active router fails, one of the Standby router will server as an active router. The HSRP Discovery Module uses cHsrpGrpTable in CISCO-HSRP-MIB to find active or standby routers.
HTTP	Protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.
HTTPS	HTTP Over SSL.
Hypertext Transfer Protocol	See HTTP .

I

ICMP	Network Layer Internet protocol that reports errors and provides other information relevant to IP packet processing.
ICMP Jitter	Allows you to generate a stream of ICMP packets between a Cisco IOS device (source) and any other IP device (destination) to gather network performance-related statistics.
Identity	<p>Identity offers authentication, access control, and user policies to secure network resources and connectivity.</p> <p>It also provides automated AAA services for switch based network access; automates security policy enforcement and provides dynamic VLAN provisioning.</p>
IDU	Incremental Device Update. Provides software updates and device updates for the earlier releases of a product.
IGMP	Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to an adjacent multicast router.
IIS	Component of the Windows Operating System that makes it easy to publish information and bring business applications to the Web.
Inactive State	In LMS, this state indicates that LMS has stopped polling for the device MIB variable instance.
Incremental Device Update	See IDU .
In Service Software Upgrade	See ISSU .
Install Mode - Software Distribution	Method of software distribution used by Software Management. According to this mode, the IOS Software Modularity image is extracted or uncompressed to a compact flash with a well defined directory structure. This mode can accommodate the point fix capabilities of Software Modularity.
instance	LMS object or element that belongs to a given device or device group.
Integration Utility	<p>Depending on the specific NMS, this utility can launch Cisco network management applications, browse Cisco MIBs, integrate traps, and add Cisco device icons to NMS topology maps.</p> <p>It also allows remote integration between CiscoWorks applications residing on one server and an SNMP management platform residing on another server.</p>
Internet Control Message Protocol	See ICMP
Internet Control Message Protocol Jitter	See ICMP Jitter .

Internet Group Management Protocol	See IGMP .
Internet Information Services	See IIS .
Internet Protocol	See IP .
Internet Protocol Version 6	See IPv6 .
interval	See duration .
inventory	<ol style="list-style-type: none"> 1. List of all of the network elements in the repository of a domain manager, and the relationships between those elements. The inventory includes devices and their components. 2. In-memory, object-oriented data structure of LMS that stores information about the managed elements currently in a network, and the relationships between these elements.
Inventory Management	<p>Inventory, or the Inventory Collection Service (ICS) and Poller software component of LMS, collects inventory data from the network devices and updates the inventory.</p> <p>If any changes are detected in hardware or software components, the inventory database is updated and a change audit record is created to inform the network manager of the change, and to document the event. This ensures that the information displayed in the Inventory reports reflects the current state of network devices.</p>
IP	Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP allows you to address type-of-service specification, fragmentation and reassembly, and security.
IP Address	<p>32-bit address assigned to hosts using TCP/IP. An IP Address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number.</p> <p>The network and subnetwork numbers together are used for routing, while the host number is used to address an individual host within the network or subnetwork.</p> <p>A subnet mask is used to extract network and subnetwork information from the IP Address. CIDR provides a new way of representing IP Addresses and subnet masks. See also IP.</p>
IP Phone Acquisition	Process that collects information about the IP Phones connected in the network.

IPSLA	Internet Protocol Service Level Agreement. This was formerly known as SAA. A portfolio of technology embedded in most devices that run Cisco IOS software. This allows you to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages.
IPSLA Availability	A dashboard which displays information such as Operation Types, Number of Collectors and Availability percentage ranges.
IPSLA Responder	Component embedded in a target Cisco device running version 12.1 or later of the Cisco IOS software. It responds to IPSLA request packets from a source device and provides accurate results.
IPv6	Replaces the IP version 4. IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).
ISSU	LMS supports In Service Software Upgrade process that allows Cisco IOS software images to be updated without rebooting the device. This increases network availability and reduces downtime caused by planned software upgrades.

J

JacORB	Object Broker Services provided and used by LMS.
Java Runtime Environment	See JRE .
Jitter	Inter-packet delay between any two consecutive data packets sent between the source and target router.
job	Reports that are scheduled to run at a later time.
Job Approval	<p>Jobs can be scheduled by the various LMS applications such as NetConfig, Config Editor, Archive Management, and Software Management. Job Approval allows you to designate one person in a group of users as a Job Approver who will approve each job before it runs.</p> <p>When Job Approval is enabled, applications that use it, require a job to be scheduled to run in the future, instead of immediately. Job approval cannot be enabled for jobs that run immediately.</p> <p>Job Approval is also referred to as Maker Checker.</p>
Job browser	<p>Central place to manage all jobs in LMS.</p> <p>The job management tasks include view the list of jobs, view the details of a selected job, stop a job and delete a job.</p>
Jobs and Resources Manager	See JRM .

Join Window	Join window is the period during which DHCP requests are processed by the SI director.
JRE	Also known as Java Runtime, consists of the Java virtual machine, the Java platform core classes, and supporting files. It is the runtime part of the Java Development Kit that does not have a compiler, debugger, or tools. It is the smallest set of executables and files that constitute the standard Java platform.
JRM	Jobs and Resources Manager. Allow applications to schedule an activity, track job instances, lock or unlock resources, and send notifications.

K

KDC	Kerberos Key Distribution Center. A centralized server used to authenticate CiscoWorks users and applications when integrated, using the secret key cryptography.
Kerberos	Developing standard for authenticating network users. Kerberos offers two key benefits. It functions in a multivendor network, and it does not transmit passwords over the network.
Kerberos Key Distribution Center	See KDC .
Kerberos Login	One of the non-ACS login modules in CiscoWorks. See also Kerberos .
KeyStore	See TrustStore .

L

LAN Management Solution	See LMS .
last configuration change	Device Troubleshooting report displays the time when the running configuration was archived in the Configuration Archive and the differences between the two archived running configurations in the Configuration Archive, under this head.
latency	Time taken for a packet to travel from the source to target and back. It is also referred to as RTT (Round-Trip Time).
layouts	Manner in which the portlets are arranged in a view.
LDAP	Lightweight Directory Access Protocol. Protocol that allows access to management and browser applications that provide read/write interactive access to the X.500 Directory.
legend	Explains the use of icons and colors in network views. Legends are available for Topology Services and Path Analysis in LMS.

Lightweight Directory Access Protocol	See LDAP .
link ports	Ports connected to Cisco devices (Switch or Router) are link ports. See also trunk port .
Link Registration	Adding additional links to CiscoWorks homepage for Custom tools and home grown tools, and third party applications such as HPOV. The links appear under the Third Party or Custom Tools, as you specify them.
Live Graph-It	Portlet that enables you to do real-time monitoring for any MIB variable that belongs to a device that is managed by DCR.
LMS	Software solution bundle that provides applications to configure, administer, monitor, and troubleshoot a network. It enables network administrators to effectively manage their LAN and campus networks.
LMS Portal	<p>CiscoWorks LMS Portal is the first page that appears when you launch the LMS application. It serves as an interface, launch point and top-level navigation for the frequently used functions in the application.</p> <p>You can view the important statistics and details of the LMS applications installed on your CiscoWorks Server, in a single page instead of navigating through several pages to view the required data.</p>
Local NMS	Network Management System on the local CiscoWorks Server. See also NMS .
local server	Identifies the CiscoWorks Server on which the Server Setup workflow is run.
local upgrade	Process of upgrading to a newer version of CiscoWorks software on the same machine.
local user setup policy	<p>Username and password policies for CiscoWorks local users in LMS.</p> <p>This policy allows to start the local username with a number, include special characters in local username, and specify the length of the local username and the local user password.</p>
log level settings	You can set the LMS log level settings. You can set the log level to Error, Fatal, Warn (Default), Info, or Debug. The log file, LMS log, is stored at <code>/var/adm/CSCOpX/log</code> on Solaris, and <code>NMSROOT/log</code> on Windows.
Logrot	Log rotation program in CiscoWorks. Rotates log when CiscoWorks is running or when the logs have reached a particular size. Optionally archives and compresses the rotated logs.
Lookup Analyzer	Utility in LMS to calculate efficiency of the DNS server.
loose source routing	IP source routing in which the IP address of the next router can be one or more routers away (multiple hops). The alternative is strict source routing, in which the next router must be adjacent (single-hop).
Low Impact Mode	Low Impact Mode enables differentiated access through policy-driven downloadable access control lists (DACLS), based on user identity information.

M

MAC Move/Replace	<p>MAC Move allows movement of non-Cisco phones or other intermediary devices that cannot signal a link-down event.</p> <p>MAC Replace is a corrective action for the security violation that is triggered when one host replaces another authenticated host.</p>
MACUHC	MAC User-Host Information Collector. Tracks wired end users dynamically. It receives MAC notification traps from the switches. If the traps are from valid sources, it updates the LMS database, accordingly.
major acquisition	Process that discovers all the End hosts and IP Phones that are connected to the devices managed by LMS.
manage Auto Smartports	In LMS, you can use this task to enable or disable auto smartports functionality on a port.
manage servers	Sub-step in the Server Set up workflow. LMS allows you to add servers You can add servers, create System Identity Users, and modify the Device Management mode. See also Server Setup .
managed device	Devices are managed in LMS when they are a part of Data Collection and are shown in Topology maps. See also Data Collection .
managed object	Network element that is monitored by a domain manager.
Managed Sourced Interface	Configures the source router with appropriate IP address to send or receive the IPSLA (Internet Protocol Service Level Agreement) operation packets.
Management Information Base	See MIB .
management state	<p>Indicates whether a device is currently being monitored.</p> <p>If a device management state is set to True, it will be discovered and monitored. If its discovery state is set to False, it will not be monitored. See also suspend and resume.</p>
Management Station to Device	Device diagnostic tool that helps you to diagnose the connectivity problems of un-managed or non-responding devices in the network.
ManagementIP Address	IP Address to access the device. One of the variables used to create and edit a group rule and a device search rule.
MD5	Message digest algorithm. MD5 is a secure hashing function that converts an arbitrarily long data stream into a digest of fixed size (16 bytes).
MDC Support Utility	Multi Domain Controller Support Utility. A diagnostic tool provided by LMS to collect the information such as database files, core client registry files, schema files, webserver configuration files, event logs, host environment information, and installation logs for debugging.

MDF Package	Meta Data Framework Package. This package defines device types in a uniform way across CiscoWorks applications. This package contains new device types, new device type definitions, new device icons, and solutions to some problems in earlier MDF packages.
MIB	<p>Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands. This is usually through a GUI network management system.</p> <p>MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.</p>
minor acquisition	Minor acquisition happens on a device if there are changes in port state, VLAN information, End hosts/IP Phones connected to the device.
Minute reports and graphs	LMS generates these reports and graphs that contain statistical data for a single or a group of collectors on a minute basis.
Missed cycles	<p>In LMS, Missed cycles is the number of polling interval cycles missed during polling.</p> <p>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.</p> <p>If the polling cycle that started at 10.00 a.m. does not complete before 10:15 a.m., then the next polling cycle will start only at 10:30 a.m. The polling cycle missed at 10:15 is called Missed Cycle.</p>
Monitoring dashboards	Provides summarized information about the health of the network.
Monitor Mode	Monitor Mode enables authentication without enforcing any kind of authorization.
MPIDS	Maintenance End Point ID's
MPLS interface	Interface on which MPLS traffic is enabled.
MPLS VPN	<p>IP network infrastructure that provides private network services over a public infrastructure. It does this by using a Layer 3 backbone.</p> <p>If you use MPLS VPNs in a Cisco IOS network you can deploy and administer scalable Layer 3 VPN backbone services including applications, data hosting network commerce, and telephony services to business customers.</p> <p>For an MPLS VPN solution, an MPLS VPN is a set of provider edge routers that are connected by a common backbone network to supply private IP inter-connectivity between two or more customer sites for a given customer.</p> <p>Each VPN has a set of provisioning templates and policies and can span multiple provider administrative domains (PADs).</p>

Multiple Authentication (Multi-auth) Mode	Multi-auth host mode allows only one client in the voice VLAN and multiple authenticated clients in the data VLAN.
Multiple Domain Authentication (Multi-domain)	Multi-domain authentication mode allows an IP Phone (Cisco or non-Cisco) and a PC to authenticate on the same switch port while it places them on appropriate voice and data VLANs.
Multiple Host Mode	Multiple host mode supports multiple hosts to authenticate on the same port in a single domain.
Multiprotocol Label Switching Virtual Private Network	See MPLS VPN .

N

NAM	A network traffic data source.
name resolution	Process of associating a name with a network location.
name server	Server connected to a network that resolves network names into network addresses.
NAR	Definition created by ACS Administrative Users in ACS. CiscoWorks must meet the conditions in the definition to access the network.
NAS	Network Access Server. A Cisco platform that interfaces with the packets and the circuit (PSTN).
Natted LMS IP Address	<p>Outcome of Network Address Translation (NAT) support in LMS. When the LMS server is assigned an IP Address that is within a NAT boundary, all the devices that are outside this boundary, cannot reach the LMS server using the inside address of the LMS server.</p> <p>For such devices, LMS must use the correct outside address of its server for these transfers. To do this, LMS allows the configuration of this outside address of its server (called Natted LMS IP Address) for each device.</p>
NDG	Collection of AAA clients such as servers and network devices. When integrating CiscoWorks Server with ACS Server, you should add the CiscoWorks Server and the devices managed in CiscoWorks under a network device group.
NetConfig	<p>NetConfig allows you to make configuration changes to your network devices, whose configurations are archived in the Configuration Archive.</p> <p>It also provides easy access to the configuration files for all LMS supported devices.</p>
Netscape Directory	One of the non-ACS login modules in CiscoWorks. Implements Lightweight Directory Access Protocol.

NetShow	<p>Commands that represent a set of read-only commands. They can either be run from the Graphical User Interface (GUI) or from the Command Line Interface (CLI).</p> <p>These are primarily, show commands that you can run on devices that are managed in LMS. LMS ships system-defined NetShow Command Sets. You cannot edit or delete any of these Command Sets.</p>
NetView	<p>Third party Network Management System to which CiscoWorks applications, icons, MIBs, and traps can be integrated.</p>
Network Access Restrictions	<p>See NAR.</p>
Network Access Server	<p>See NAS</p>
Network Administrator	<p>Predefined role in CiscoWorks applications. Can perform all Network Operators tasks. Can perform tasks that result in a network configuration change.</p>
Network Device Group	<p>See NDG.</p>
Network File System	<p>See NFS.</p>
Network Management Integration Module	<p>See NMIM (Also known as Integration Utility).</p>
Network Management System	<p>See NMS.</p>
Network Operator	<p>Predefined role in CiscoWorks applications. Can perform tasks related to network data collection. Cannot perform any task that requires write access on the network.</p>
New Technology File System	<p>See NTFS.</p>
NFS	<p>Network File System. It is a distributed file system protocol suite developed by Sun Microsystems that allows remote file access across a network.</p>
N-Hop view	<p>Displays a N-hop view from a specified device. This is much faster than the regular Campus Manger Topology services and should be used to view a limited set of devices.</p>
NMIM	<p>See Integration Utility.</p>
NMS	<p>System responsible for managing at least part of a network. Typically, an NMS is a reasonably powerful and well-equipped computer such as an engineering workstation. NMSs communicate with agents to track network statistics and resources.</p>

NMSROOT	Directory where CiscoWorks LMS is installed.
Non Installed Mode - Software Distribution	<p>Method of software distribution used by Software Management. This process involves distributing images by copying the IOS Software Modularity images to the hard disk of the device, updating the boot commands, and rebooting the OS on the device.</p> <p>You can run the Cisco IOS Software Modularity Images in this mode and so it is also called IOS Software Modularity non-install mode. It is also known as binary mode.</p>
non-link trunk ports	Trunk ports connected to End hosts or IP Phones. See also trunk port .
Not Reachable	In LMS, Not Reachable status indicates that the device may be down or not reachable.
notifications	Configurable messages sent by LMS to certain recipients. Notifications are configured by type (e-mail, syslog, SNMP trap) and group (certain events, devices, alerts, severity, status, etc.) A notification subscription consists of a notification type, a notification group, and a set of recipients.
NTFS	Windows NT file system used to organize and keep track of files.
NV RAM	Non-Volatile Memory where the start-up configuration in a device is stored.
<hr/>	
O	
Object identifier	See OID .
Object Finder portlet	Helps you to extensively search, sort, and filter functions and to query the managed entities. You can view the device details, the job details, the End Host details, (MAC, IP address, host name, and device names, user name). You can also view the online help details.
Object Grouping Service	See OGS .
Object Grouping Service Command Line Interface	See OGSCLI .
ODBC	Generic vendor independent API for accessing relational databases.
OGS	Service provided by LMS to group objects such as devices and collectors.
OGSCLI	Interface used to export groups information to a file and import groups information from a file to server.
OID	Object identifier. Uniquely identifies a device, module, interface, or power supply. Values are defined in specific MIB modules.
Open Database Connectivity	See ODBC .

Open Shortest Path First Protocol See [OSPF](#).

operation Set of parameters used to measure network performance statistics. The parameters specify the type of measurement to be performed and many other parameters specific to the type of measurement being taken.

OpsxmlDbEngine Database engine for the LMSLMS workflow engine.

OpsXMLRuntime Cisco Works Assistant workflow engine.

osagent Process that allows CORBA servers to register their objects and assists CiscoWorks applications in the location of objects.

OSPF One of the Discovery protocols supported by Device Discovery.

The OSPF Discovery Module uses ospfNbrTable and ospfVirtNbrTable MIB to find its neighbor's IP addresses.

Out-of-Sync report Depicts the startup configuration, running configuration and the diff (difference) between the two configurations for selected group of devices. It summarizes the configuration details of the devices whose running and startup configurations are not synchronized.

Overlay graph Comparative view of the latency of one or more collectors.

P

Package Map List of all device packages installed on a CiscoWorks Server maintained by Software Center.

Package Support Updater See [PSU](#).

Packet Capture Device diagnostic tool that can be used to capture the live data from the CiscoWorks Server and troubleshoot the problems in the server.

Packet Loss Measures the total number of packets lost while moving from source to target and back.

PAK Product Authorization Key. A key printed on the label of LMS Bundle product box. You should use this key to register your software and obtain a product license.

PAM Pluggable Authentication Module for CiscoWorks Server, such as Active Directory, Kerberos Login and so on.

panner Displays a compact view of the entire Network Topology view.

Parent group Container groups and the groups that have sub-groups.

Path Analysis	Diagnostic application that traces the connectivity between two specified devices in the network, including the physical and logical paths taken by packets flowing between those points.
path echo	Measures end-to-end and hop-by-hop network response time between a Cisco device and other devices using IP. Path Echo is available only for the IP protocol.
Peer Server Account	User accounts set up on a CiscoWorks Server. This account can enable communication among multiple CiscoWorks Servers. This can also authenticate processes running on a remote CiscoWorks Server.
Peer Server Certificate	<p>Certificate of peer CiscoWorks Servers. This is required to communicate with another CiscoWorks Server in a domain.</p> <p>When you add a server using Server Setup workflow, LMS fetches the certificate information of the server you are adding, and prompts you to accept the peer certificate. See also Trust creation.</p>
Performance Tuning Tool	See PTT .
PERL	Unix based scripting language. Perl scripts ends with an extension.pl
Permanent	In LMS, Permanent status is displayed if the polled MIB variables or instances are not available in the device.
Permissions report	Report in LMS that provides information on roles, and privileges associated with the roles. It specifies the tasks that a user in a particular role can perform.
PID	Process ID. A unique number by which the operating system identifies each running program on a CiscoWorks Server.
PIN	Place of the device in the network layer (Edge, Core, Access, Distribution)
Ping	Device diagnostic tool used by CiscoWorks. Use the Ping tool to test whether the device is reachable. A Ping tests an ICMP echo message and its reply.
Ping sweep	Basic network scanning technique used to determine which range of IP addresses map to live end hosts.
PKCS	Set of standards for public-key cryptography developed by RSA Laboratories. These standards are designed for binary and ASCII data.
PKI	System of certificate authorities, registration authorities and other supporting agents. These authorities perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.
Pluggable Authentication Module	See PAM .

PMCOGSServer	<p>Process that is required for administering Port and Module Groups in LMS.</p> <p>You can start this process using Admin > System > Server Monitoring > Processes. In the Process Management page, select the PMCOGSServer and click Start.</p>
PoE	<p>Power over Ethernet or technology is a system to transfer electrical power, along with data, to remote devices over standard twisted-pair cables in an Ethernet network.</p> <p>The terms power over Ethernet (PoE), power over LAN (PoL), and inline power are synonymous terms used to describe the powering of attached devices through Ethernet ports.</p>
POE Port Level report	In LMS, this report displays information such as power consumption, power available and power remaining at the port level for devices. See also Power Policing .
PoE Port Utilization report	In LMS, this report displays the power utilization for each device polled for the Power Over Ethernet Port Utilization template. See also Power Policing .
PoE PSE Consumption report	In LMS, this report displays the power utilization for each device polled for the Power Over Ethernet PSE Consumption template. See also Power Policing .
POE report	<p>Power over Ethernet (POE) is the ability of the LAN switching infrastructure to provide power over a copper Ethernet cable to an endpoint (Powered device).</p> <p>You can generate the POE report in LMS. See also Power Policing.</p>
poll interval	Periodicity for polling the network using Device Poller. See also Device Poller .
Poller	Collection of devices and template MIB instances.
Poller reports	In LMS, these are reports created, based on the template added in a given Poller
polling frequency	Indicates how often CiscoView sends SNMP queries to a managed device.
Polling interval	<p>Frequency at which the server polls the source router to retrieve the statistics and update the database. LMS retrieves the data from source router every hour by default.</p> <p>The polling interval (such as 1, 5, 15, 30, or 60 minutes) is specified while creating collectors. The default polling interval is 60 minutes.</p>
Polling parameter	Displays the edited parameters for the selected device group.
Port and Module Configuration	LMS allows you to create groups based on ports and modules for a selected set of devices or device groups. You can do this using Port and Module Group Administration.
port attributes	Information about the ports in a device such as, Type of port, Administrative Status.
Portal Log Settings portlet	Sets the level of details you will find in the log based on the settings you configure.

portlets	Enables you to organize information inside a view. These are user interface components that are managed and displayed in a view.
Power over Ethernet	See Power Policing
Power Policing	<p>Task that allows you to configure Power and Power Policing in ports.</p> <p>Power Policing allows you to turn off power while generating Syslogs. This is needed if the real-time power consumption exceeds the maximum power allocation on the port.</p> <p>Power policing and PoE is supported only on Catalyst 3750-E and Catalyst 3560-E switches with PoE ports. This task is available only in the Port based flow of a NetConfig job.</p>
Power Sourcing Equipment	See PSE .
Primary ACS server	Primary server providing authentication services to CiscoWorks Server after integration. If the primary server is down, authentication services are provided by secondary servers, if they are configured.
Primary credentials	Primary values used to access the devices in the network. Primary credentials are stored in DCR. You can use secondary credentials to access the devices if you cannot access them using primary credentials.
Privacy password	SNMPv3 privacy password of the device in AuthPriv mode.
Privacy protocol	SNMPv3 privacy algorithm used in AuthPriv mode. Can be DES, 3DES, AES128, AES192, and AES256.
Private	LMS Portal can be a public portal or private portal. In the Private mode you can customize and configure the Views and Portlets. To select Private Portal, go to CiscoWorks LMS Portal and select Private at the top right corner.
Product Authorization Key	See PAK .
Product Instance Device Mapping	Registry that stores mapping information between devices and applications. Also, known as PIDM. Each CiscoWorks application should register the information about the devices with PIDM.
Provider Edge router	Router on the border between a VPN provider and a VPN customer that belongs to the provider
Proxy server	Intermediate server that connects the clients to the external server.
PSE	Power Sourcing Equipment refers to network devices (switches or hubs for instance), that will provide power in a Power over Ethernet (PoE) setup. See also PoE .
PSIRT	Cisco's Product Security Incident Response Team.

PSIRT Summary report	<p>Inventory report, generated based on the PSIRT information retrieved from Cisco.com at regular intervals. This report helps you to ascertain the security vulnerabilities that affect the devices in your network.</p> <p>It provides a summary of the possible security alerts based on the selected devices. It also recommends upgrade to the IOS image version that has the fix for the security vulnerability.</p>
PSU	<p>Central location within the CiscoWorks application to check for software updates and device updates, download and install the updates, and schedule downloading updates.</p>
PSUCLI	<p>CLI version of Package Support Updater.</p>
PTT	<p>Performance Tuning Tool. Command Line Interface (CLI) utility that enables you to apply and list various profiles available in CiscoWorks Server. Profiles consists of configuration files in the form of XML files whose values are based on the recommendations for various applications.</p>
Public Key Cryptography Standards	<p>See PKCS.</p>
Public Key Infrastructure	<p>See PKI.</p>
Public mode	<p>LMS Portal can be a Public or a Private portal. In the Public mode you can view all the portlets added by the Administrator. You can select the portal as Public to view only the portlets added into the Public portal by the administrator.</p>

Q

QoS	<p>Measure of performance for a transmission system that reflects its transmission quality and service availability.</p>
Quality of Service	<p>See QoS.</p>
Quick reports	<p>LMS contains a set of predefined system generated reports called Quick reports.</p> <p>Quick reports provide detailed information on the top 10 and bottom 10 devices polled by LMS. These are devices that have the highest or lowest utilization or availability value.</p>

R

RA	<p>Authority in a network that verifies the digital certificate submitted by a requestor.</p>
-----------	---

RADIUS	Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time. One of the non-ACS login modules available in the CiscoWorks Server.
Range operator	Operator for group rule or search rule expressions. Enables you to group the devices of the specified range of IP Addresses. You can select the range operator only for the <i>ManagementIpAddress</i> variable. You should enter the range of IP Addresses in the Value field.
RCP	Protocol that allows you to copy files to and from a file system residing on a remote host or server on the network. The rcp protocol uses TCP to ensure the reliable delivery of data.
RCP user	Name used by network device when it connects to CiscoWorks Server to run RCP. User account must exist on UNIX systems, and should also be configured on devices as local user in the <code>ip rcmd configuration</code> command
Readiness report	Provides information about the VRF readiness of the devices. The Readiness report enables administrators to identify VRF Capable, VRF Supported and other devices on a network.
Reachable	In LMS, this indicates that the device is available and reachable in the network.
Reachable devices	Devices that are discovered by Device Discovery.
Really Simple Syndication	See RSS .
Real-time graph	Allows you to monitor the statistics of a collector on a real-time basis.
refresh rate	Indicates how often a monitoring dialog box is updated by CiscoView. The default value is 30 seconds.
Registration Authority	See RA .
Regular Server	See RS .
Remote Authentication Dial-In User Service	See RADIUS .
Remote Copy Protocol	See RCP .
Remote Monitoring	See RMON .
Remote NMS	Network Management System on the remote CiscoWorks Server. See also NMS .
Remote upgrade	Process of installing a newer version of CiscoWorks software on a different machine and restoring the data backed up from the older version to the newer version.

report archives	Report is archived when a scheduled report job has completed successfully and stored in archive for future reference.
report granularity	Level of detail in a report that you want to view from the archived statistics. The various levels available are Minute, Hourly, Daily, Weekly, and Monthly.
report job	Jobs for which reports are scheduled to run at the specified date and time.
Report Job Browser	<p>In LMS, Report Job Browser allows you to view the list of report jobs scheduled to generate reports. From the Report Job Browser, you can perform report job management activities such as viewing the details of a report job, deleting a report job, suspending a report job, resuming a report job and viewing a report.</p> <p>System jobs are not shown in the Report Job Browser.</p>
Reports	LMS offers comprehensive reporting on the data collected by polling the device and presents this data using tables and graphs. These reports help network administrators analyze the utilization and availability of devices connected to the network. Reports also provide the historical trending information of a device.
Request/Response Unit	See RU .
restore data	See database restore .
resume	Setting a device management state to True so that LMS will monitor the device. This is normally done from the Detailed Device view. See also suspend .
retry	Number of times CiscoView will send an SNMP request to a managed device before the request times out.
System-defined groups	Default grouping of devices. This is a read only group. You cannot create new groups under system-defined groups. The system-defined device groups available in LMS are All Devices, Normal devices, Pre-deployed, Previous selection and Saved device list.
RMON	<p>Remote monitoring. MIB agent specification described in RFC 1271 that defines functions for remote monitoring networked devices. The RMON specification provides monitoring, problem detection, and reporting capabilities.</p> <p>Download the CiscoView Mini-RMON Manager device package to enable RMON functionality within CiscoView.</p>
Rogue MAC	MAC Addresses that are not authorized to exist in your network.
root device	Device from which the N-Hop portlet starts drawing the Topology map.
round-trip time	See RTT .
Round-trip time monitor management information base	See RTTMON MIB .
route	Path through an internetwork between a specific source and target.

Route Processor	See RP .
router	Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another, based on network layer information.
Route Distinguisher	Number that identifies VPNs in the provider's (MPLS) network and it supports overlapping address in a network. Route distinguisher is prefixed to private IPv4 addresses to make the IPv4 addresses globally unique. The value is used by the edge router to identify the VPNs to which packets belongs to. For example: A PE router can distinguish between the IP address 10.10.10.1 of one customer from the 10.10.10.1 of another customer, the network administrator must add a unique route distinguisher to each.
Routing Control Processor	See RCP .
RP	Route Processor. Processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. Sometimes called a supervisory processor.
RS	Single Sign-On Slave server using the authentication services from the Master. The regular server should be configured in the same domain as the Master server.
rsh	Remote Shell Protocol. Protocol that allows you to run commands on a remote system without logging into the system.
RSS	Really Simple Syndication. XML-based format used to distribute Web content (such as news headlines). By using RSS, web content publishers can easily create and disseminate current news headlines and URLs.
RTT	Time required for a network packet to travel from the source to the destination and back. RTT includes the time required for the destination to process the message from the source and generate a reply. The latency measurements taken by LMS and SA Agent are round-trip time latency measurements.
RTTMON MIB	Proprietary MIB created by Cisco to obtain and store round-trip time statistics. The MIB is implemented by the Cisco IOS software in the source router. LMS obtains the round-trip time statistics from this MIB. This MIB has been extended to monitor network performance statistics in addition to round-trip time statistics.
RU	Request and response messages exchanged between NAUs in an SNA network.

S

SAA	Feature of Cisco IOS software that allows you to measure and monitor network performance between a Cisco router and a remote device.
------------	--

SA Agent Responder	<p>Component embedded in a target Cisco router running version 12.1 or later of the Cisco IOS software. It responds to SA Agent request packets from a source router running the SA Agent software.</p> <p>The Responder can listen on any user-defined port for UDP and TCP protocols. The SA Agent Responder is required only for specific collector types, such as Enhanced UDP for monitoring jitter in Voice-over-IP networks.</p>
Sample Interval	<p>Frequency with which the source device polls the target device to retrieve the statistics based on the IPSLA operations configured by you. LMS retrieves the statistics from the target device every 60 seconds, by default.</p>
scheduled report	<p>See job.</p>
SCP user	<p>Name used by network device when it connects to CiscoWorks Server to run SCP.</p> <p>The username you have entered here is used for authorization while the device transfers software images, using SCP protocol.</p>
search rule	<p>Consists of one or more rule expressions combined by logical operators. Used to filter and display only the devices that satisfy the rule conditions, in the device selector.</p>
Secondary ACS Server	<p>ACS server that provides authentication services to CiscoWorks Server only when the primary ACS server is down. You should configure the hostname or IP Address, and the port number on the CiscoWorks Server.</p>
secondary credentials	<p>Credentials that you can use as a fallback if you cannot access the network devices using primary credentials. Secondary credentials comprise a username, a password, and a console-enabled password for the devices.</p>
secret key	<p>Text string (usually passwords) used in a multi-server domain to maintain the confidentiality and provide authenticity among the servers.</p>
Secure Hash Algorithm	<p>See SHA.</p>
Secure Shell	<p>See SSH.</p>
Secure Socket Layer	<p>See SSL.</p>
security certificate	<p>Similar to digital ID cards. They prove the identity of the server to clients. certificates are issued by Certificate Authorities (CAs) such as VeriSign or Thawte.</p>
Security mode	<p>In Identity, you can choose the level of security you wish to implement in the selected switches.</p>
seed device	<p>Starting point for Device Discovery. See also Device Discovery.</p>
seed file	<p>A text file that lists top-level network devices (for example, hosts, routers, and switches) by name or IP address, and the read community strings of the devices. LMS can use seed files to initiate device discovery.</p>

selective backup	<p>Saving only the selected data and configuration files to maintain a safe copy.</p> <p>See also database backup.</p>
Self-Signed certificate	<p>Security certificates created on the CiscoWorks Server that enable SSL communication between the client browser and management server. Self-signed certificates are valid for five years from the date of creation.</p> <p>When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed CiscoWorks.</p>
server	<p>Node or software program that provides services to clients.</p>
Server Setup	<p>One of the LMS workflows. It helps you to simplify the deployment and setting up of single or multiple LMS servers.</p>
Service Assurance Agent	<p>See SAA.</p>
Setup Center	<p>Centralized area that displays the LMS System configurations and allows you to configure the necessary server settings, immediately after installing LMS Software.</p>
SHA	<p>Algorithm that accepts a message of less than 264 bits in length and produces a 160-bit message digest.</p>
Show Map	<p>Shows the connectivity details of the devices on which VRF is to be configured. Using Show Map, you can view the connectivity details of up to 30 devices.</p>
Simple Mail Transfer Protocol	<p>See SMTP.</p>
Simple Network Management Protocol	<p>See SNMP.</p>
Single Host Mode	<p>Single Host mode allows only one user to authenticate per port.</p>
Single Sign On	<p>See SSO.</p>
SIU	<p>Communication between multiple CiscoWorks Servers is enabled by a trust model addressed by certificates and shared secrets. Use the System Identity setup to create a trust user on Slave servers to facilitate communication in Multi-server scenarios.</p> <p>This trust user is called System Identity User. The System Identity User is also used for inter-process communication. See also Trust creation.</p>
Smart Call Home	<p>Smart Call Home is a new, secure connected service that is currently available on the Cisco Catalyst 6500 devices. It offers proactive diagnostics and real-time alerts on select Cisco devices and provides higher network availability and increased operational efficiency.</p>

SmartCase	Lets you access Cisco.com from LMS to open a Cisco.com case or to query and update an existing case. It allows you to submit, review, and update problems or questions about Cisco products.
Smart Install	Smart Install (SI) is a plug-and-play configuration and image management feature that provides zero-touch deployment for new switches.
Smart Install Groups	You must define a minimum of one Smart Install group to configure an SI director.
Smartports	In LMS, you can use this task to apply smartports on a port by selecting the predefined smartports macros.
SMTP	Simple Mail Transfer Protocol. Internet protocol providing e-mail services.
SNMP	Simple Network Management Protocol. It is used almost exclusively in TCP/IP networks. SNMP allows you to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. CiscoView supports SNMP versions 1, 2, and 3.
SNMP agent	Simple Network Management Protocol agent. Resides in the source router and is provided as part of Cisco IOS software. The SNMP agent receives requests from the SNMP server to perform all LMS-related functions.
SNMP community string	Text strings that act as passwords to authenticate messages sent between the network management station and devices containing an SNMP agent. Community strings allow you to limit access to network devices.
SNMP MAC notification	MAC address notification enables you to track users on a network. Whenever the switch learns about or removes a MAC address, an SNMP notification can be generated and sent.
SNMP retries	Number of attempts made to query the device.
SNMP Set	Device diagnostic tool that allows you to set an SNMP object or multiple objects on a device for controlling the device.
SNMP timeout	Time period after which the SNMP query times out.
SNMP trace	Displays information on SNMP requests sent by CiscoView to managed devices.
SNMP Traps Forwarding	Forwards SNMP traps from devices in the LMS inventory. LMS will forward the raw trap in the format in which it was received from the device. All traps are forwarded in V1 (SNMP Version) format.
SNMP Traps Receiving	Receives SNMP traps on port 162 (or, if port 162 is occupied, port 9000).
SNMP walk	Device diagnostic tool that allows you to trace the MIB tree of a device starting from a given OID for troubleshooting or to gather information about a certain device.
SNMPv3	Version 3 of SNMP.

Software Center	Helps you to check for software and device support updates, download them to their server file system along with the related dependent packages, and install the device updates. Also known as PSU.
SoftWare Image Management	See SWIM .
Software Management CLI	Command-line Interface of LMS. You can use this tool to invoke the Software Management features from the command-line.
source device	Devices which support IPSLA and which performs the operations by generating packets at the predefined intervals and storing the measured values.
source router	Originating router or switch running IOS from which LMS measures network performance. The source router or switch must be running a version of Cisco IOS software version that supports IPSLA.
source-route bridging	See SRB .
SQL	International standard language to define and access relational databases.
SRB	Method of bridging originated by IBM and popular in Token Ring networks. In an SRB network, the entire route to a destination is predetermined, in real time, before the data is transmitted to its destination.
SRE Operation	<p>In LMS, you can use the SRE Operation task to perform the following operations in the service modules of SRE supported devices:</p> <ul style="list-style-type: none">• Install application in service modules• Uninstall application from service modules• Understand:<ul style="list-style-type: none">– Status of the service module– Application that is running on the module– Status of the current installation in the service module– Status of uninstallation in the service module• Stop the installation on a set of service modules in a SRE device• Reset service modules in a SRE device• Shutdown the set of service modules in a SRE device
SSCP	Focal point within an SNA network to manage network configuration, coordinate network operator and problem determination requests, and provide directory services and other session services for network end users.
SSCP-PU session	Session used by SNA to allow an SSCP to manage the resources of a node through the PU. SSCPs can send requests to, and receive replies from, individual nodes to control the network configuration.
SSH	Protocol that provides a secure remote connection to devices. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in the Cisco IOS software.

SSL	Encryption technology for the Web used to provide secure transactions. CiscoWorks uses SSL to provide secure access between the client browser and the management server.
SSO	Single Sign On enables you to use your browser session to transparently navigate to multiple CiscoWorks Servers without authenticating to each of them.
SSO mode	<p>The SSO authentication server is called the Master, and the SSO regular server is called the Slave. Authentication always takes place from the SSO Master server (Authentication Server-AS).</p> <p>Authorization happens at the respective servers. The CiscoWorks Server can also be configured to be in the Standalone mode (Normal mode, without SSO). See also SSO.</p>
SSP	Protocol specified in the DLSw standard, used by routers establish DLSw connections, locate resources, forward data, and handle flow control and error recovery. See also DLSw .
Stack Group	This is a custom group which is used to set up the image and configuration file for all client switches that match stack number for switches in a stack.
stale groups	Groups that belongs to users groups who are removed from CiscoWorks.
Standby Switch	After converting two VSS-enabled Standalone Switches into a Virtual Switching System, one switch becomes the Standby Switch and other the Active Switch.
static group	Group whose membership is refreshed only when you explicitly request it. Between re-evaluations, the Group Server stores the membership list and group definition of the static group. Whenever you view a Static group, you can see the membership list that the ASA created the last time the group rule was evaluated.
static route	Explicitly configured route entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols.
Structured Query Language	See SQL .
Sub Interface	Logical interfaces derived from a physical interface.
subnet based acquisition	<p>Runs only on those subnets that are configured in LMS.</p> <p>LMS discovers End Hosts and IP Phones on all VLANs in the configured subnets.</p>
subnet groups	<p>System defined device group in device selector that contains the devices managed in LMS.</p> <p>These subnet based groups help you work on smaller subsets of devices that are logically grouped.</p>
subscription	See notifications .

Super Admin	User in LMS created after the CiscoWorks Server is integrated. Cperform all CiscoWorks operations including the administration and approval tasks. By default, this role has full privileges.
suspend	To set a device's management state to False so that LMS will not monitor the device. This is normally done from the Detailed Device View. See also resume .
SWIM	<p>Software Image Management or Software Management in LMS automates the steps associated with upgrade planning, scheduling, downloading software images, and monitoring your network.</p> <p>It provides tools that make it easier to store backup copies of all Cisco software images running on network devices. It also helps to store any additional software images if required, and to plan and run software image upgrades to multiple devices on the network at the same time.</p>
Switch Check	<p>You can select this while running the End Host Down/IP Phone Down workflow. If you select this option, LMS will check the reachability status for the selected device to which the End Host is connected.</p> <p>Otherwise, it will check the reachability status for the Cisco Call Manager (CCM) to which the IP Phone is connected. See also End Host/IP Phone Down.</p>
Switch-to-Switch Protocol	See SSP .
Syslog Analyzer/Collector	Allows you to centrally log and track syslog messages (error, exception, information etc.) sent by devices in the network. You can use the logged message data to analyze network device performance. You can also customize this application to store and produce important information.
Syslog messages	<p>Messages that originate from a device in response to some activity that affects it. The devices that are connected to the LMS server, are configured to send Syslog messages to the LMS Syslog server whenever there are changes.</p> <p>The LMS server receives these messages either directly from the devices in the network or through a Remote Syslog Collector installed in the network. You can use these logged Syslog messages to analyze network device performance.</p>
Syslog Receiver Group	Group of hosts that receives Syslog messages when any TrendWatch or Threshold violation occurs in LMS. LMS allows you to create Syslog Receiver Groups using the Syslog Receiver Groups option.
syslogConf.pl Utility	<p>Perl Script CLI utility. You can use this to Change Syslog Analyzer Port, Change Syslog Collector Port, Configure Remote Syslog Collector (RSAC) Address and Port in LMS server, and Change Syslog File Location.</p> <p>You can run this script in the LMS server as well as on the RSAC server. You can perform all these tasks on a LMS server by running the syslogConf.pl script from the command prompt.</p>
System Administrator	Predefined role in CiscoWorks. Can perform all CiscoWorks system administration tasks.

System-defined group	Top-level container for standard groups that are accessible to and used by most LMS users. It is available by default.
System Identity User	See SIU .
System Services Control Point	See SSCP .
System status	Details about LMS processes—Device Discovery, Data Collection and User Tracking Acquisition.
System view	View that contains all system related portlets, such as Job Information Status portlet, DCR and AAA, Log Space Usage, and Process Status.
System-defined template	<p>In LMS, System-defined MIB templates provide most of the common network parameters that you need to monitor a device connected to the network.</p> <p>These templates cannot be deleted or modified.</p>

T

TAC	Cisco's Technical Assistance Center.
TACACS	<p>Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging.</p> <p>User passwords are administered in a central database instead of in individual routers, providing an easily scalable network security solution. See also TACACS+ in the Cisco Systems Terms and Acronyms section.</p>
TACACS+	Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting. See also TACACS in main glossary.
target device	<p>Device to which the packets are sent by the IPSLA source devices. Target devices are the destination devices for which you want to gather network performance statistics.</p> <p>The target devices can be any IP-addressable device or a Cisco device running the IPSLA Responder on which the source router performs IPSLA operations.</p>
TCP	Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack. See also TCP/IP .
TCP/IP	Common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite. See also TCP and IP .

TDR	Time Domain Reflectometry (TDR) is used to detect faults in a cable. TDR checks and locates open circuits, short circuits, sharp bends, crimps, kinks, impedance mismatches, and other such defects.
Template	In LMS, this is a collection of MIB variables logically grouped by the user or the system to monitor the utilization and availability levels of a device (such as CPU, memory, interface).
Template Center	<p>Template Center in LMS provides you with a list of both system-defined templates and user-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.</p> <p>You can modify the system-defined templates and save them as user-defined templates. You can also import templates from a client machine and these templates are stored as user-defined templates in LMS.</p>
Template management	Allows you to create a user-defined template, modify the configuration of a user-defined template, export and import a user-defined template, delete a user-defined template, and so on.
Terminal Access Controller Access Control System	See TACACS .
Tertiary ACS Server	ACS server that provides authentication services to CiscoWorks Server only when both the primary ACS server and the secondary ACS server are down. You should configure the hostname or IP Address, and the port number in CiscoWorks Server.
TFTP	Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication. For example, username and password.
Threshold	In LMS, this is an optimal value for a MIB variable set by the user or the system.
Threshold setup	Threshold rule can be set for only one MIB variable at a time and you can set many thresholds for each MIB variable. You can set threshold rules for all the MIB variables on a device selected for polling.
Threshold Violation reports	In LMS, these are reports created, based on the threshold configured for the MIB variable.
Time Domain Reflectometry reports	Detects faults in a cable. LMS supports TDR Cable Diagnostic Test and generates a report listing the results of the test on Cisco Catalyst 6000 switches.
timeout	<p>Event that occurs when one network device expects to hear from another network device within a specified period of time, but does not. Typically, a timeout results in a retransmission of information, or the cancellation of the session between the two devices.</p> <p>In CiscoView, this is the length of time that elapses before an SNMP request sent by the application to a managed device times out.</p>

TOC	Table of Contents.
Tomcat	Java servlet engine used on Windows and Solaris systems that hosts applications on the CiscoWorks desktop.
Topology and Neighbor information	LMS features that let you manage, view, and monitor the physical and logical services on your network. You can also get information on neighbor devices.
Topology filters	Filters devices, links, and networking services. Locates these items on the Network Topology Views.
Topology groups	Customized views, of the network in which devices are grouped according to various criteria. A view may be considered as a group of devices or device elements.
Topology Services	Messages about the status of Topology Services that appear on the left side of the status bar. These messages typically are displayed at the start and end of a task that is performed within Topology Services.
Traceroute	Device diagnostic tool used to detect routing errors between the management station and the target device. Helps you understand why ping fails or why applications time out.
Transient	In LMS, this status is displayed if the device is down or the SNMP credentials are incorrect.
Transmission Control Protocol	See TCP .
Transmission Control Protocol/Internet Protocol	See TCP/IP .
trap	Message sent by an SNMP agent to an NMS, console, or terminal indicating that a significant event has occurred. This could be a specifically defined condition or a threshold that has been reached.
Trap listener	LMS server port that listens to SNMP MAC Notification traps sent from devices.
Trap Receiver group	Group of hosts that receives specified trap notifications, when any TrendWatch or Threshold violation occurs in LMS. LMS allows you to create SNMP Trap Receiver Groups using the Trap Receiver Groups option.
TrendWatch	Allows you to continuously monitor a value over time, sampling the value at periodic intervals to view the trends.
TrendWatch report	LMS report that is created based on the TrendWatch configured for the MIB variable. You can create, edit, copy, and view these reports for specific TrendWatch MIB variables.
Trivial File Transfer Protocol	See TFTP .

trunk port	Switch port that is connected to another Layer 2 device (such as a switch or bridge). This is by default, a member of all VLANs that exist on the switch and carry traffic for all VLANs, among the switches.
Trust creation	Creation of trust is required to enable communication between CiscoWorks Servers part of a multi server set up. Communication among multiple CiscoWorks Servers is enabled by a trust model addressed by Certificates and shared secrets. See also Peer Server Certificate and System Identity User .
TrustStore	Also known as KeyStore. The location where CiscoWorks maintains the list of certificates that it trusts.

U

UDF	Stores additional information about a device in DCR. DCR supports a maximum of ten UDFs. By default, the DCR Administration user interface provides four UDFs.
UDP	Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.
UDP jitter	User Datagram Protocol jitter. It allows you to measure round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic.
UDM	Unified Device Manager (UDM) provides centralized device management using a centralized policy configuration. You have to configure a single policy to manage the devices. UDM identifies managed devices after verifying the configured policy and the license count.
UE	User Experience.
UI	User Interface.
unacknowledging discrepancy	Returns an acknowledged discrepancy into the Discrepancies report. See also acknowledging discrepancy .
Uniform Resource Locator	See URL .
Uniform Resource Name	See URN .
unreachable devices	Devices that are not reachable by LMS Device Discovery.
UPN	User Principal Name. It is composed of two parts, User login and UPN suffix. You should enter the User login name and UPN suffix for a UPN-based authentication to MS Active Directory Server.

URL	Type of formatted identifier that describes the access method and the location of an information resource object on the Internet.
URN	<ol style="list-style-type: none">1. Uniform Resource Name. An Internet addressing scheme.2. Refers to the URL of a AUS Managed Device in CiscoWorks.
User Datagram Protocol	See UDP .
User Datagram Protocol jitter	See UDP jitter .
User-defined fields	See UDF .
User-defined group	Top-level container where individual application users can create their own groups. Typically, the groups under User Defined Groups are used and accessible to the user who created the group, and perhaps a small group of additional users. Groups created by you, based on the device attributes in DCR
User Principal Name	See UPN .
User Tracking	Allows you to track End Hosts and IP Phones connected to the network.
User Tracking utility	Allows you to search for users or hosts discovered by User Tracking application. Comprises a server-side component and a client utility.
User-defined template	<p>LMS allows you to create your own templates. You can do this by grouping new MIB variables or by leveraging MIB variables from an existing System-defined template to suit your requirements. These templates are called user-defined templates.</p> <p>You can add or delete MIB variables in a user-defined template.</p>
UT major acquisition	See major acquisition .
utilization	Percentage of a particular resource, such as CPU or memory, currently in use by a device, card, or port, as indicated by a CiscoView monitoring dialog box.
UTLite	Process that collects user names from Primary Domain Controllers, Active Directory, and Novell servers. It runs only on Windows clients.
UTManager	Process that receives information from MACUHIC about newly added end hosts in the network. This information is completed using updates from DHCP or UTLite or from both. See also MACUHIC .

V

Virtual Local Area Network	See VLAN .
Virtual Routing and Forwarding	See VRF-Lite .
Virtual Switching System	<p>Technology that combines two standalone distribution switches found in the local distribution layer into a single management point.</p> <p>The Virtual Switching System functions and appears as a single switch to the wiring closet and the core layer. You can also create Virtual Switching Systems with a pair of standalone switches available in the core layer.</p>
Virtual Switching System Configuration	Process of converting two VSS-enabled Standalone distribution switches into a Virtual Switching System. Virtual Switching System Configuration Tool available in LMS is used to convert the two VSS-enabled Standalone Switches into a Virtual Switching System.
Virtual Switching System Configuration tool	The Virtual Switching technology is implemented in LMS by providing a Virtual Switching System Configuration Tool. This GUI based conversion tool allows you to select two compatible standalone switches and guides you to convert those standalone switches into one Virtual Switching System.
Virtual Switching System Mode	When two Standby switches are converted to a Virtual Switching System, they are considered to be in Virtual Switching System Mode.
virtualization	Allows you to run multiple virtual machines with same or different Operating Systems independently on the same physical machine.
VLAN	<p>Virtual Local Area Network. This is a group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire. This is although they are located on a number of different LAN segments.</p> <p>VLANs are based on logical instead of physical connection. This makes them extremely flexible.</p>
VMware	Virtualization system on which CiscoWorks LMS can be installed and run.
voice trace	Specifies Voice over IP (VoIP) traffic trace between telephone number.
VoIP Call Setup Post Dial Delay	Measures network response time for setting up a VoIP call.
VoIP Gatekeeper Registration Delay	Allows you to measure the average, median, or aggregated network response time of registration attempts from a VoIP gateway to a VoIP gatekeeper device.
VoIP RTP	Real-Time Transport Protocol (RTP)-based Voice over IP (VoIP) operation allows you to set up and schedule a test call and use Voice gateway digital signal processors (DSPs) to gather network performance-related statistics for the call.

VRF	VPN routing or forwarding instance. A VRF includes the routing information that defines a VPN site that is attached to a PE router. This can be an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of routing protocols that determine what goes into the forwarding table.
VRF Based report	Displays the VRF details specific to the VRFs selected while generating the report. See also VRF-Lite .
VRF Capable Devices	Represents the devices with necessary hardware support. To configure VRF on these devices, you need to update the software of the device.
VRF Collection	Fetches the complete information about the VRFs from the network. See also VRF-Lite .
VRF-Lite	One of the simplest form of implementing virtualization technology in an Enterprise network. A Virtual Routing and Forwarding is defined as VPN routing/forwarding instance. A VRF consists of an IP Routing table, a derived forwarding table, a set of interfaces that use the forwarding table and set of routing protocols that determine what goes into the forwarding table.
VRF Supported Devices	Represents the devices with necessary hardware and software support to configure VRF.
VSS Configuration	See Virtual Switching System Configuration .
VSS Mode	See Virtual Switching System Mode .

W

WLSE UHIC	Process that updates the LMS database with the information on wireless clients. WLSE UHIC polls the Wireless LAN Solution Engines (WLSE) periodically and receives details on the changes occurring in the wireless host associations.
Work Centers	Work Centers in LMS 4.0 provides complete lifecycle management of Identity, EnergyWise, Auto Smartports, and Smart Install from Day 1 to Day N operations in a workflow-oriented approach. This includes readiness assessment, configuration, monitoring, and reporting capabilities.
workflows	LMS workflows help you to deploy and manage the CiscoWorks Servers and troubleshoot your network. The workflows take you through the different steps required to achieve these tasks. You can perform the steps required to set up a multi-server set up, in a single flow. Also, you can generate device troubleshooting reports that use features from the different installed applications, without having to go to each of them to run the tasks. See also End Host/IP Phone Down , Device Troubleshooting and Server Setup .

X

- XML** Standard maintained by the World Wide Web Consortium (W3C). It defines a syntax that lets you create markup languages to specify information structures. CiscoWorks maintains application configuration, roles, tasks and other information in XML format.
- XSL** XML Stylesheets.