



Installing and Getting Started With CiscoWorks LAN Management Solution

Software Release 3.1

CiscoWorks

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

Text Part Number: OL-16574-01

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0805R)

Installing and Getting Started With CiscoWorks LAN Management Solution 3.1
Copyright © 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

SUPPLEMENTAL LICENSE AGREEMENT ix

Notices xiii

OpenSSL/Open SSL Project xiii

License Issues xiii

Preface xvii

Audience xvii

Conventions xvii

Product Documentation for LAN Management Solution 3.1 xviii

Related Documentation for LAN Management Solution 3.1 xix

Obtaining Documentation, Obtaining Support, and Security Guidelines xxi

CHAPTER 1

Overview of LAN Management Solution 3.1 1-1

Product Overview 1-1

Composition of LAN Management Solution 3.1 1-2

Key Features of LMS 3.1 1-4

Install and Upgrade Behavior 1-4

Support for New Server and Client Operating Environments 1-7

Support for New Hardware in LMS 3.1 1-7

Removal and Upgrade of Third Party Components 1-7

Auto Allocation of Devices to Applications 1-8

Enhancements to Report Jobs 1-10

Enhancements to Job Settings in Reports 1-11

Support for Zone-based Virtualization in Solaris 10 1-11

Support for ZFS File System 1-11

Support for LDom Virtualization 1-11

Supported Network Management Systems 1-12

Supported Devices 1-13

CHAPTER 2

Prerequisites 2-1

System and Browser Requirements for Server and Client 2-2

Operating System Requirements 2-3

Server Requirements on Solaris Systems 2-4

Server Requirements on Windows Systems 2-6

System Requirements on Client Servers	2-8
Terminal Server Support for Windows 2003 Server	2-9
Solaris Patches	2-10
LAN Management Solution Port Usage	2-13
Required Device Credentials for LMS Applications	2-16

CHAPTER 3

Preparing to Install CiscoWorks LAN Management Solution 3.1 3-1

Terms and Definitions Used in LMS Installation Framework	3-1
Before You Begin Installation	3-3
License Information	3-5
Application Scaling Numbers	3-7
Standalone Server	3-7
Solution Server	3-7
Concurrent Users Supported	3-8
Licensing Your Product	3-8
Installing the Licensing File	3-11

CHAPTER 4

Performing Installation of LAN Management Solution 3.1 4-1

Performing New Installation of LMS 3.1	4-2
Installing LMS 3.1 on Solaris - New	4-2
Installing LMS 3.1 on Solaris —New (Typical)	4-6
Installing LMS 3.1 on Solaris — New (Custom)	4-9
Installing LMS 3.1 on Windows - New	4-14
Installing LMS 3.1 on Windows — New (Typical)	4-17
Installing LMS 3.1 on Windows —New (Custom)	4-20
Installing LMS 3.1 in Silent Mode	4-23
Upgrading to LMS 3.1	4-25
Local Upgrade to LMS 3.1 on Solaris	4-26
Local Upgrade to LMS 3.1 on Solaris — Typical	4-28
Local Upgrade to LMS 3.1 on Solaris — Custom	4-32
Remote Upgrade to LMS 3.1 on Solaris	4-36
Local Upgrade to LMS 3.1 on Windows	4-37
Local Upgrade to LMS 3.1 on Windows — Typical	4-39
Local Upgrade to LMS 3.1 on Windows — Custom	4-42
Remote Upgrade to LMS 3.1 on Windows	4-46
Verifying the Installation	4-47
Uninstalling LMS 3.1	4-49
Before You Begin Uninstallation	4-49

Uninstalling LMS 3.1 on Solaris	4-50
Uninstalling LMS 3.1 on Windows	4-51
Re-installing LMS 3.1	4-52

CHAPTER 5

Getting Started with LAN Management Solution 3.1 5-1

Before You Start	5-2
Accessing CiscoWorks Server	5-2
Logging Into the CiscoWorks Server	5-3
Understanding the CiscoWorks LMS Portal Home Page	5-3
CiscoWorks LMS Portal Home Page	5-3
Views	5-6
Portlets	5-7
Launching LMS Applications	5-8
Launching LMS Workflow Demos	5-8
Configuring LMS Administration Parameters	5-9
Using LMS Setup Center	5-9
System Setup and Administrative Tasks	5-10
Setting Up CiscoWorks Server	5-15
Before You Begin CiscoWorks Server Setup	5-15
Understanding Single-Server and Multi-Server Setup	5-15
Understanding DCR and Device Management	5-16
Understanding Single Sign-On	5-21
Understanding AAA Modes	5-21
About CiscoWorks Assistant	5-22
Methods of Deploying CiscoWorks Server Setups	5-22
Setting Up a Single CiscoWorks Server	5-24
Manage LMS Server	5-24
Set up Device Management Mode	5-25
Set up Default Credentials	5-26
Add Devices	5-27
Manage Devices in the Applications Installed in the LMS Servers	5-32
Setting Up Multiple CiscoWorks Servers	5-35
Terms and Definitions	5-35
Before Setting Up Multi-Servers	5-36
Multi-Server Setup Tasks	5-37
Integrating CiscoWorks Server with ACS	5-40
CiscoSecure ACS Support	5-40
CiscoWorks Server Authentication Roles	5-41
Before You Begin ACS Integration	5-42

Setting Up ACS Server	5-42
Changing the AAA Mode to ACS Using the Server Setup Workflow	5-43
Assigning Roles to Users and User Groups In ACS	5-45
Impact of Installing CiscoWorks Applications in ACS Mode	5-45
Verifying LMS Applications and the Cisco Secure ACS Configuration	5-46
Managing Devices in CiscoWorks Server	5-46
Managing Devices and Credentials	5-46
Managing Devices in CiscoWorks Applications	5-47
RME Device Management Using cwcli Inventory Command	5-47
Adding Adhoc Target Devices to IPM	5-47
Preparing to Use LMS Applications	5-48
Preparing to Use Campus Manager	5-48
Processes and Settings	5-48
Data Collection Settings	5-49
User Tracking Settings	5-49
Starting Topology Services	5-50
Configuring SNMP Trap Listener for Dynamic UT to Work in Campus	5-50
Preparing to Use Device Fault Manager	5-52
Enabling Devices to Send Traps to DFM	5-52
Integrating DFM Trap Receiving with NMSs or Trap Daemons	5-53
Updating the SNMP Trap Receiving Port	5-54
Configuring SNMP Trap Forwarding	5-54
Preparing to Use Internetwork Performance Monitor	5-55
IPM Application Settings	5-55
Auto Allocation Settings	5-56
Managing IPM Operations	5-56
Working With Collectors	5-57
Preparing to Use Resource Manager Essentials	5-58
Setting Up Inventory	5-59
Setting Up Syslog Analyzer	5-59
Setting Up Software Management	5-61
Setting Up Configuration Management	5-63
Preparing to Use Health and Utilization Monitor	5-63
Creating a Poller	5-64
Creating a Threshold	5-64
Creating a Template	5-64
Using CiscoView	5-65
Using CiscoView Mini-RMON Manager	5-65
Using Device Center	5-65
Launching Device Center	5-66

Invoking Device Center	5-66
Using Integration Utility	5-67
Performing Maintenance on Your CiscoWorks Server	5-67
Performing Regular Backups	5-67
Purging the Data	5-69
Maintaining the Log Files	5-71
Using CiscoWorks LMS Applications Online Help	5-71

CHAPTER 6**Troubleshooting and FAQs 6-1**

Checking Processes After Installation	6-1
Viewing and Changing Process Status	6-1
Troubleshooting Your Network Using CiscoWorks Assistant	6-3
Generating Device Troubleshooting Report	6-3
Generating End Host Down/IP Phone Down Report	6-4
Contacting Cisco Technical Assistance Center (TAC)	6-4
Understanding Installation Error Messages	6-5
Frequently Asked Questions	6-13

APPENDIX A**User Inputs for Installation A-1**

User Inputs for Typical Installation	A-2
User Inputs for Custom Installation	A-3
Password Information	A-7
Password Rules for New Installation	A-7
Password Rules for Upgrade Installation	A-7
Password Rules for Re-installation	A-7
Password Descriptions	A-7
CiscoWorks Admin Password	A-8
System Identity Account Password	A-8
CiscoWorks Guest Password	A-8
LMS Application Database Password	A-8
Changing CiscoWorks Admin Password	A-8
Changing casuser Password	A-9

APPENDIX B**User Tracking Utility B-1**

Understanding UTU 1.1.1	B-1
Definitions	B-2
Hardware and Software Requirements for UTU 1.1.1	B-2
Downloading UTU 1.1.1	B-3

Installing UTU 1.1.1	B-3
Accessing UTU 1.1.1	B-5
Configuring UTU 1.1.1	B-6
Searching for Users or Hosts	B-6
Using Search Patterns	B-9
Uninstalling UTU 1.1.1	B-9
Upgrading to UTU 1.1.1	B-10
Re-installing UTU	B-11

APPENDIX C

Installing the Remote Syslog Collector	C-13
Verifying Remote Syslog Collector Server Requirement	C-14
Installing the Remote Syslog Collector	C-15
Installing on Solaris	C-15
Installing on Windows	C-16
Subscribing to a Remote Syslog Collector	C-16
Starting the Remote Syslog Collector	C-17
Stopping the Remote Syslog Collector	C-17
Uninstalling the Remote Syslog Collector	C-17
Uninstallation on Windows	C-17
Uninstallation on Solaris	C-18
Understanding the Syslog Collector Properties File	C-18

INDEX

SUPPLEMENTAL LICENSE AGREEMENT

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CISCOWORKS LAN MANAGEMENT SOLUTION

IMPORTANT—READ CAREFULLY: This Supplemental License Agreement ("SLA") contains additional limitations on the license to the Software provided to Customer under the Software License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the Software License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download, or otherwise use the Software. When used below, the term "server" refers to central processor unit.

ADDITIONAL LICENSE RESTRICTIONS

Device Restricted Versions. Customer may install and run the Software on a single server to manage up to the device count specified in the Right-To-Use statement located on the Claim Certificate received as part of the software package. When used anywhere in this SLA, a "device" means any device in the Customer's network environment which has its own IP address. Please refer to this guide for further device definition.

Customers whose requirements exceed the restricted version limit of devices must purchase another license or upgrade to a higher device support version of the Software. Device restrictions are enforced by license registration and through serial key installation.

Limitations associated with the maximum number of devices an application can support per server is specified below. Please refer to this guide for further device definition. Device restrictions are enforced by license registration and through serial key installation. The licensed device limit will always override the maximum number of devices supported per server unless the customer has purchased and registered the 10,000 device license offering.

Installation and Use

The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Some license terms, such as device count and proof of preexisting licenses may be electronically enforced. Customer may install and use the following Software components:

- CiscoWorks Common Services with CiscoWorks Assistant, CiscoWorks LMS Portal and CiscoWorks CiscoView: Contains shared resources used by other components in this solution. In many cases, all components in this solution can be installed on a single server. If some components of this solution are installed on separate servers, a copy of CiscoWorks Common Services, CiscoWorks Assistant and CiscoWorks LMS Portal can be installed with each component in the Customer's network management environment.
- CiscoWorks Resource Manager Essentials (CiscoWorks RME): May be installed on one (1) server in Customer's network management environment. Maximum device support is 10,000 per server. Installing the Software and applying a single serial license key to more than two (2) servers is supported in the 10,000 device restricted version but the cumulative total number of devices supported cannot exceed 10,000 per serial license key.

- CiscoWorks Campus Manager (CiscoWorks Campus): May be installed on one (1) server in Customer's network management environment. Maximum device support is 5,000 per server. Installing the Software and applying a single serial license key to more than two (2) servers is supported in the 10,000 device restricted version but the cumulative total number of devices supports cannot exceed 10,000 per serial license key.
- CiscoWorks Device Fault Manager (CiscoWorks DFM): May be installed on one (1) server in Customer's network management environment. Maximum device support is 5,000 per server. Installing the Software and applying a single serial license key to more than two (2) servers is supported in the 10,000 device restricted version but the cumulative total number of devices supports cannot exceed 10,000 per serial license key.
- CiscoWorks Internetwork Performance Monitor (CiscoWorks IPM): May be installed on one (1) server in Customer's network management environment. Maximum device support is 5,000 devices and 5000 collectors per server. Installing the Software and applying a single serial license key to more than two (2) servers is supported in the 10,000 device restricted version but the cumulative total number of devices the version supports cannot exceed 10,000 devices and 5000 collectors per serial license key. For CiscoWorks IPM alone the license will be based on the number of devices and the number of collectors.

Additional Information for 5,000 Device Restricted Version for LMS 3.1

- Users of CiscoWorks LMS 3.1 with 5,000 device restricted licensing may require individual CiscoWorks LMS applications, such as CiscoWorks DFM, or CiscoWorks RME, to be run on separate servers in order to support a large number of devices or to meet certain performance criteria.
- More than one copy of CiscoWorks applications may be installed on secondary servers provided the customer has purchased and registered the 5,000 device restricted version of the CiscoWorks LMS software. When installed on secondary server, the cumulative total number of devices supported cannot exceed 5,000 per serial license key. Device support beyond 5,000 will require additional licenses and copies of CiscoWorks LMS to be purchased.
- When more than one server is used to host CiscoWorks LMS, each server should have a copy of the original license key installed on it. Customers should not modify the license file.
- Legal restriction concerning the distribution of the CiscoWorks LMS applications is described in the Supplemental License Agreement.

Additional Information for 10,000 Device Restricted Version for LMS 3.1

- Users of CiscoWorks LMS 3.1 with 10,000 device restricted licensing often require individual CiscoWorks LMS applications, such as CiscoWorks DFM, or CiscoWorks RME, to be run on separate servers in order to support a large number of devices or to meet certain performance criteria.
- More than one copy of CiscoWorks RME, CiscoWorks Campus Manager, CiscoWorks DFM and CiscoWorks IPM may be installed on a secondary servers provided the customer has purchased and registered the 10,000 device restricted version of the CiscoWorks LMS software. When installed on secondary server, the cumulative total number of devices supported cannot exceed 10,000 per serial license key. Device support beyond 10,000 will require additional licenses and copies of CiscoWorks LMS to be purchased.
- When more than one server is used to host CiscoWorks LMS, each server should have a copy of the original license key installed on it. You should not modify the license file.

- Legal restriction concerning the distribution of the CiscoWorks LMS applications is described in the Supplemental License Agreement.

Reproduction and Distribution

Customer may not reproduce nor distribute software.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

Please refer to the Cisco Systems, Inc. Software License Agreement.



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:

© 1998-1999 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:

© 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].



Preface

This guide helps you to understand and use LAN Management Solution 3.1 effectively. It is a guide that will help you in the software installation on both Windows and Solaris as well as help you get started with using the product.

This guide also provides you with some troubleshooting suggestions that may be useful while you work on LAN Management Solution 3.1 software.

Audience

This guide is for anyone who installs, upgrades, configures, verifies, and uses LAN Management Solution 3.1 software. Network administrators or operators should have the following skills:

- Basic Windows or Solaris system administrator skills.
- Basic network management skills.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	<code>screen</code> font
Information you enter	boldface <code>screen</code> font
Variables you enter	<i>italic</i> <code>screen</code> 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.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Product Documentation for LAN Management Solution 3.1

**Note**

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

Table 1-1 describes the product documentation that is available.

Table 1-1 Product Documentation

Document Title	Available Formats
<i>Installing and Getting Started with CiscoWorks LAN Management Solution 3.1 (this document)</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html
<i>Data Migration Guide for CiscoWorks LAN Management Solution 3.1</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html
<i>Supported Devices Tables of RME, CM, CV and DFM (LMS 3.1)</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM. On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html

Related Documentation for LAN Management Solution 3.1


Note

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

Table 1-2 describes the additional documentation that is available.

Table 1-2 **Related Documentation**

Document Title	Available Formats
<i>User Guide for CiscoWorks Common Services 3.2</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html
<i>User Guide for Campus Manager 5.1 (With LMS 3.1)</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps563/products_user_guide_list.html
<i>User Guide for Resource Manager Essentials 4.2 (With LMS 3.1)</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_user_guide_list.html
<i>User Guide for Device Fault Manager 3.1 (With LMS 3.1)</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps2421/products_user_guide_list.html
<i>User Guide for Internetwork Performance Monitor 4.1 (With LMS 3.1)</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps1008/products_user_guide_list.html

Table 1-2 **Related Documentation (continued)**

Document Title	Available Formats
<i>User Guide for CiscoView 6.1.8</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps4565/products_user_guide_list.html
<i>User Guide for CiscoWorks LMS Portal 1.1</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/ps7198/products_user_guide_list.html
<i>User Guide for CiscoWorks Assistant 1.1</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/ps7212/products_user_guide_list.html
<i>User Guide for Health and Utilization Monitor 1.1</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://cisco.com/en/US/products/ps9303/products_user_guide_list.html
<i>User Guide for CiscoWorks Integration Utility 1.7</i>	<ul style="list-style-type: none"> PDF on: <ul style="list-style-type: none"> Product DVD LMS 3.1 Documentation CD-ROM On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

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.



CHAPTER 1

Overview of LAN Management Solution 3.1

This chapter provides a clear overview of CiscoWorks LAN Management Solution 3.1 and describes the composition of LAN Management Solution 3.1 on both Windows and Solaris systems.

This chapter contains:

- [Product Overview](#)
- [Composition of LAN Management Solution 3.1](#)
- [Key Features of LMS 3.1](#)
- [Supported Network Management Systems](#)
- [Supported Devices](#)

Product Overview

The LAN Management Solution (LMS) 3.1 software provides applications for configuring, administering, monitoring, and troubleshooting a campus network. It enables network administrators to effectively manage their LAN and Campus networks.

This document describes the procedure for a new and upgrade installation of LMS 3.1. It contains:

- LMS product composition, including links for accessing online documentation.
- LMS features.
- Hardware and software requirements.
- Detailed installation procedures for all applications.
- Information on getting started with LMS.
- Frequently asked questions.
- Information about ordering documentation and contacting Cisco Systems for additional assistance.

If you already have an earlier version of LMS and want to migrate to LMS 3.1, follow the procedure in the *Data Migration Guide for LAN Management Solution 3.1*.

You can find this document at this URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html

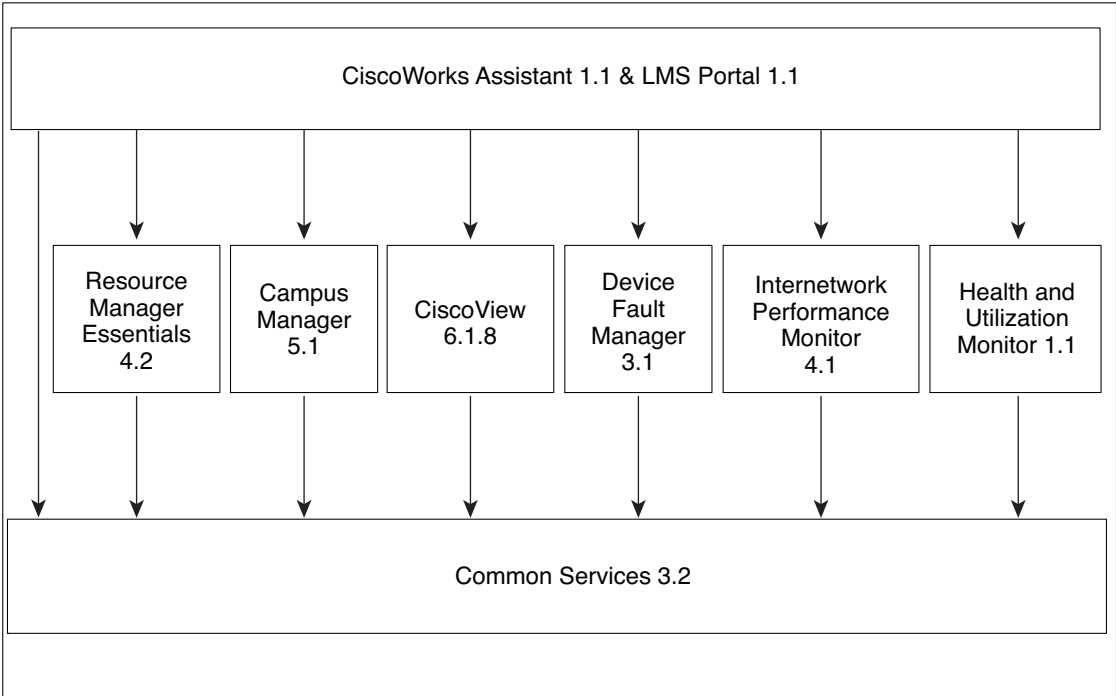
The licenses in LMS 3.1 are device-based for all applications. However, for Internetwork Performance Monitor (IPM) the license is based on the number of devices and the number of collectors.

Based on the requirement, you can select the appropriate license. See [License Information](#) for further information.

Composition of LAN Management Solution 3.1

The LAN Management Solution 3.1 software is packaged in a DVD for your use. [Figure 1-1](#) explains the composition of LAN Management Solution 3.1 software.

Figure 1-1 *Composition of LAN Management Solution 3.1*



271180

The entire list of applications comprised within LAN Management Solution 3.1 has been tabulated below.

You can select to upgrade install any number of applications based on your need and the system prerequisites. However, CiscoWorks Common Services 3.2, CiscoWorks Assistant 1.1 and CiscoWorks LMS Portal 1.1 will be selected and installed by default.

Table 1-1 describes the composition of applications within LAN Management Solution 3.1.

Table 1-1 Composition of Applications within LAN Management Solution 3.1

This LMS 3.1 Application...	Provides...
CiscoWorks Common Services 3.2 (CS)	Common software and services for LMS applications. Common Services provides a set of shared application services that are used by all LMS applications.
Resource Manager Essentials 4.2 (RME)	The ability to manage: <ul style="list-style-type: none"> • Device inventory and audit changes. • Configuration files, software images, and syslog analysis. • Network monitoring and fault information for tracking devices that are critical to network uptime.
Campus Manager 5.1 (CM) Campus Manager is sometimes referred to as Campus.	The following functions: <ul style="list-style-type: none"> • Visualize network topology. • Locate and display data about users and hosts in the network. • Manage VLANs. • Detect network discrepancies and Best Practice Deviations
CiscoView 6.1.8 (CV)	The ability to monitor and troubleshoot devices across your network being a graphical device management tool.
Device Fault Manager 3.1 (DFM)	The following functions: <ul style="list-style-type: none"> • Monitor device faults in real-time, and determine the root cause by correlating device-level fault conditions. • Monitor fault history. • Configure e-mail, SNMP trap, and syslog notifications.
Internetwork Performance Monitor 4.1 (IPM)	The ability to pro-actively troubleshoot network response time, jitter, and availability.
CiscoWorks LMS Portal 1.1	The ability to: <ul style="list-style-type: none"> • Customize information, based on the applications installed. • View frequently used information in a common place. With this you do not need to navigate through many pages. • Display application-related information as portlets. • Customize home page to have all information on a single screen from all the installed applications.
CiscoWorks Assistant 1.1	Workflows to: <ul style="list-style-type: none"> • Set up and manage CiscoWorks LAN Management Solution (LMS) servers. • Collect troubleshooting information.

Table 1-1 **Composition of Applications within LAN Management Solution 3.1 (continued)**

This LMS 3.1 Application...	Provides...
CiscoWorks Health and Utilization Monitor 1.1	Monitors the device for performance parameters, report violations based on the threshold values configured, and provides extensive reporting.
Integration Utility 1.8 (NMIM)	Support for third-party Network Management Systems (NMS). This is an integration module.

Key Features of LMS 3.1

The following are the key features of LMS 3.1:

- [Install and Upgrade Behavior](#)
- [Support for New Server and Client Operating Environments](#)
- [Support for New Hardware in LMS 3.1](#)
- [Removal and Upgrade of Third Party Components](#)
- [Auto Allocation of Devices to Applications](#)
- [Enhancements to Report Jobs](#)
- [Enhancements to Job Settings in Reports](#)
- [Support for Zone-based Virtualization in Solaris 10](#)
- [Support for ZFS File System](#)
- [Support for LDom Virtualization](#)
- [Supported Network Management Systems](#)

See the respective application User Guides to know about the key features of all LMS applications.

Install and Upgrade Behavior

LMS 3.1 provides a single install experience to you. It allows you to select and install all applications together or select specific applications.

The complete installation is managed by this single installer. It captures all required user inputs and then installs the applications.

The evaluation version of HUM 1.1 is packaged with LMS3.1, and is a part of the single installer. Since HUM has a separate license, during installation, you are prompted to first enter the license information for LMS3.1 and then for HUM 1.1.

For complete details on installation, see [Performing Installation of LAN Management Solution 3.1](#).

This section contains the following topics:

- [Upgrade and Migration Overview](#)
- [Upgrading Master-Slave Server Setup](#)

Upgrade and Migration Overview

Upgrading is overwriting the existing LMS version with the new LMS version. LMS 3.1 enables you to upgrade from an earlier version of LMS and perform a fresh installation of other applications at the same time.

When you install LMS 3.1, the existing applications of LMS are selected by default for upgrading to the latest version of LMS 3.1.

For example, if you had installed Resource Manager Essentials 4.0.5 (LMS 2.6) previously, and when you now install LMS 3.1 using the DVD, this application will be selected by default for an upgrade installation to Resource Manager Essentials 4.2 (LMS 3.1).

The three default applications namely, CiscoWorks Common Services 3.2, CiscoWorks Assistant 1.1 and CiscoWorks LMS Portal 1.1, will also be selected.

The other applications you want to install can also be simultaneously selected for a fresh installation, using the LMS 3.1 DVD.

You can upgrade using either of these methods:

- Local upgrade—Upgrading to the newer version of LMS on the same machine.
You can locally upgrade to LMS 3.1 from LMS 3.0, LMS 3.0 December 2007 update, LMS 2.6 and LMS 2.6 Service Pack (SP) 1.
- Remote upgrade—Installing LMS on a different machine and then restoring the data on that machine.
You can do a remote upgrade to LMS 3.1 from LMS 3.0, LMS 3.0 December 2007 update, LMS 2.6 and LMS 2.6 Service Pack (SP) 1.

Upgrading Master-Slave Server Setup

The Master server should be first upgraded to the latest version of LMS. Then the Slave server should be upgraded.

You can upgrade only if the Master server has a higher version of LMS (for example, LMS 3.1) and the Slave server has a lower version of LMS (for example, LMS 3.0.)

You cannot upgrade if the Master server has a lower version of LMS (for example, LMS 3.0 and the Slave server has a higher version of LMS (for example, LMS 3.1).

Table 1-2 describes the recommended sequence to upgrade, and migrate your data from earlier versions of LMS to LMS 3.1.

Table 1-2 Upgrade and Data Migration Procedure

Current LMS Version	Type of Upgrade	Procedure
LMS 3.0, LMS 3.0 December 2007 update, LMS 2.6, LMS 2.6 Service Pack 1.	Local Upgrade	<p>Upgrade to LMS 3.1 using the LMS 3.1 DVD.</p> <p>For details on the upgrade procedures, see the Upgrading to LMS 3.1.</p> <p>Data from the older version of LMS is automatically migrated into LMS 3.1 from LMS 3.0 onwards. For upgrades from LMS 2.6 / LMS 2.6 SP1, all data gets migrated to LMS 3.1 except IPM.</p> <p>To migrate IPM data, follow the instructions in the <i>Data Migration Guide for LAN Management Solution 3.1</i>.</p>
LMS 2.6, LMS 2.6 SP1, LMS 3.0, LMS 3.0 December 2007 update	Remote Upgrade	<ol style="list-style-type: none"> 1. Back up the data in the old machine. 2. Install LMS 3.1 in the new machine. 3. Migrate your data to LMS 3.1 using the instructions in the <i>Data Migration Guide for LAN Management Solution 3.1</i>.
LMS 2.2, LMS 2.5, LMS 2.5.1	Direct upgrade to LMS 3.1 is not supported. The suggested upgrade path is: LMS 2.2 / LMS 2.5 / LMS 2.5.1 > LMS 2.6 > LMS 3.1	<ol style="list-style-type: none"> 1. Back up the data. 2. Upgrade from the earlier versions of LMS to LMS 2.6 and migrate the data, using the instructions in: <ul style="list-style-type: none"> – <i>Readme for CiscoWorks LMS 2.6 Update on Solaris</i> – <i>Readme for CiscoWorks LMS 2.6 Update on Windows</i> – <i>Data Migration Guide for LAN Management Solution 2.6</i> 3. For remote upgrade from LMS 2.6, backup data for all the applications. For local upgrade from LMS 2.6, backup only the IPM data. 4. Upgrade from LMS 2.6 to LMS 3.1. 5. Migrate data using the instructions in the <i>Data Migration Guide for LAN Management Solution 3.1</i>.

Support for New Server and Client Operating Environments

Support for the following has been added in LMS 3.1:

New Server Operating Systems supported in LMS 3.1

Solaris 10, 08/07 release

New Virtualization System supported in LMS 3.1

- VMWare ESX 3.5.0
- Zone based Virtualization in Solaris 10
- Logical domains (LDoms) in Solaris 10

New Operating Environment supported in LMS 3.1

ZFS file System for Solaris 10 Operating System

Support for New Hardware in LMS 3.1

The new hardware supported in LMS 3.1 is:

- UltraSPARC T2 Processor
- VMWare Optimized hardware
 - Intel-VT processors
 - Intel® vPro™ processor technology
 - Intel® Xeon® processor 5000 sequence
 - Intel Xeon processor 7000 sequence
 - Intel Xeon processor 3000 sequence
 - Intel® Itanium® Processor 9000 sequence
 - AMD-V

Removal and Upgrade of Third Party Components

The following third party components are removed and replaced with open source components in LMS 3.1:

- Visigenics that was used for CORBA communication is replaced with JACORB.
- Tibco that was used for event services is replaced with ActiveMQ

The following component upgrade is performed in LMS3.1:

- Itools framework (Installation framework) that was scripted using Installshield 5.5 is migrated to Installshield 2008 premier version.
- Sybase ASA version is upgraded to 10.0.1 from 9.x. because 10.x has better performance.

Auto Allocation of Devices to Applications

In the previous versions of LMS, device allocation is done either in the auto or manual mode, except in Campus Manager that has filter support.

The new feature Auto Device Allocation helps you to define rules and policies and automatically allocate the devices based on the rules into various LMS applications.

Groups (System created and User-defined groups) created in Common Services are used for this purpose. Application specific groups are not be used for this.

To set up the Auto Allocation feature:

-
- | | |
|---------------|--|
| Step 1 | Create groups using Common Services Group Administration page using fields like sysLocation, ip-address range etc. |
| Step 2 | Go to each application Auto Allocation settings page and select the appropriate mode. |
| Step 3 | Add devices in DCR via Discovery, Import or Manual addition. |
- If the devices are already present in DCR, this step is not required.
-

The Auto Allocation feature can be enabled from the following menu paths in these applications:

- **Campus Manager > Admin > Data Collection > Mode and Policy Settings**
- **Resource Manager Essentials > Admin > Device Management > Device Mgmt Settings**
- **Device Fault Manager > Device Management > Device Import > Auto allocation settings**
- **Internetwork Performance Monitor > Admin > Auto Allocation Settings**

There are three possible modes in Auto Allocation:

- **Manual** — Auto allocation is disabled and you must add devices manually into each application.
- **Allocate All Devices** — Auto allocation is enabled and all the devices in DCR are added into the application. New devices added into DCR after applying the settings, will be dynamically added into applications.
- **Allocate By Groups** — Auto allocation is enabled and user can select one or more groups from Common Services. The list of devices that are part of the selected groups are added into application. New devices added into the group after applying the settings, will be dynamically added into applications.

It is possible that each application in the same LMS server can be in different modes.

For example: RME can be in Allocate All Devices mode and DFM can be in Manual mode. You can manually add devices, even if the mode is Allocate all Devices or Allocate by Groups.

For complete details of the above modes, see the User Guide of the relevant application.

This section contains:

- [Auto Allocation mode in DCR Master Slave Setup](#)
- [Behavior during Fresh Installation of LMS 3.1](#)
- [Behavior during Local Upgrade and Remote Upgrade/Restore](#)
- [Behavior During Re-installation of LMS 3.1](#)

Auto Allocation mode in DCR Master Slave Setup

If the Master Slave setup is present, then groups from Master Server will be shown in the Group selector. This occurs whether the application is installed in the Master or in the Slave machine. All functionalities will behave as in the normal standalone DCR mode.

The following are the possible DCR mode changes and the corresponding device management mode:

- DCR mode changes from Standalone to Master
Auto Allocation mode is preserved.
- DCR mode changes from Standalone to Slave
All the devices are removed from the application space and device management is set to Manual Mode.
- DCR mode changes from Slave to Standalone
Auto Allocation mode is preserved.
- DCR mode changes from Slave to Master
Auto Allocation mode is preserved.
- DCR mode changes from Master to Slave
All the devices are removed from the application space and device management is set to Manual Mode.
- DCR mode changes from Master to Standalone
Auto Allocation mode is preserved.

Behavior during Fresh Installation of LMS 3.1

The following are the settings for the applications during fresh install:

- CM and RME
Auto Allocation feature is enabled in the Allocate All Devices mode
- DFM and IPM
Auto Allocation is off and device management will be in Manual mode

Behavior during Local Upgrade and Remote Upgrade/Restore

Each application behaves differently during upgrade, based on its previous version settings.

- RME and IPM
 - If Auto Allocation was enabled in the previous version of LMS, after upgrading to LMS 3.1, the Auto Allocation feature is enabled in the Allocate All Devices mode.
 - If Auto Allocation was disabled in the previous version of LMS, after upgrading to LMS 3.1, Device Management will be in Manual mode.
- DFM
 - If Synchronization with DCR option was enabled in previous version of LMS, after upgrading to LMS 3.1, the Auto Allocation feature is enabled in the Allocate All Devices mode.
 - If Synchronization with DCR option was disabled in the previous version of LMS, after upgrading to LMS 3.1, Device Management will be in Manual mode.

- CM
 - If the filters were not specified in the Data Collection settings in the previous version of LMS, after upgrading to LMS 3.1, Auto Allocation feature is enabled in the Allocate All Devices mode.
 - If the filters were specified in the Data Collection setting in the previous version of LMS, after upgrading to LMS 3.1, Auto Allocation feature is enabled in the Allocate by Group mode.
Campus Manager automatically creates a group with the name *Migrated_From_CM_Filters*, which matches the filter criteria and this group is selected.

Behavior During Re-installation of LMS 3.1

Auto Allocation settings will be preserved during re-install.

Enhancements to Report Jobs

After the completion of report jobs, the entire report is sent as e-mail, so that you can quickly access it.

You can:

- Enable this option in the Common Services Admin page. To access this page select **Common Services > Server > Admin > System Preferences**.
- Specify the type of attachment
- Specify the maximum size of the attachment

If the attachment is larger than the specified size, the URL to launch the report is included in the e-mail.

The following reports are sent as e-mails:

- Health and Utilization Monitor — All reports
- Resource Manager Essentials
 - Inventory Reports
 - Syslog Reports
 - CDA jobs
 - Baseline Jobs Reports
- Campus Manager
 - Rogue MAC Report
 - New MAC Report
 - Dormant MAC report

Enhancements to Job Settings in Reports

While specifying time period for report generation, you can now specify whether the date range is in days, months or years. This makes the date selection much easier.

The following reports have been enhanced with this feature:

- Campus Manager
 - Switch Port Reports —Reclaim Unused Up and Reclaim Unused Down
 - MAC Reports — Rogue MAC, New MAC and Dormant MAC
 - History Reports — History Switch Port Utilization and End Host History
- Device Fault Manager—Fault History report
- Resource Manager Essentials:
 - Syslog report
 - Change Audit report

Support for Zone-based Virtualization in Solaris 10

Solaris Zones (Supported from Solaris 10) is a virtualization technology from SUN Microsystems (www.sun.com). It allows you to create isolated and secure environments called zones for running applications.

LMS3.1 will support LMS in whole-root non-global zone. Sparse root zone is not supported.

There is no specific hardware or software requirement for zone support. LMS works in the same way in non-global zones, as it works on global zone.

Support for ZFS File System

ZFS is a new kind of file system for the Solaris Operating System, based on pooled storage model. LMS 3.1 supports ZFS file system. It is supported in both global and non-global zones.

Support for LDom Virtualization

LDoms (Logical domains) is a virtualization technology from SUN Microsystems For details, see <http://www.sun.com/servers/coolthreads/ldoms/index.xml>

LDOMs are supported in LMS3.1.

Supported Network Management Systems

Table 1-3 lists the Network Management Systems (NMS) supported by Integration Utility 1.8, which is part of LMS 3.1.

Table 1-3 Supported Network Management Systems

Network Management System	Supported Platforms
HP OpenView 7.51	<ul style="list-style-type: none"> • Solaris 9 • Solaris 10 • Windows 2003 Standard Edition with Service Pack 1 • Windows 2003 Enterprise Edition with Service Pack 1 • Windows 2003 R2 Standard Edition • Windows 2003 R2 Enterprise Edition
HP OpenView 7.50	<ul style="list-style-type: none"> • Solaris 9 • Windows 2003 Standard Edition with Service Pack 1 • Windows 2003 Enterprise Edition with Service Pack 1
NetView 7.1.5	<ul style="list-style-type: none"> • Solaris 9 • Solaris 10 • Windows 2003 Standard Edition • Windows 2003 Enterprise Edition • Windows 2003 R2 Standard x64 Edition • Windows 2003 R2 Enterprise x64 Edition
NetView 7.1.4	<ul style="list-style-type: none"> • Solaris 9 • Windows 2003 Standard Edition • Windows 2003 Enterprise Edition

See *User Guide for CiscoWorks Common Services 3.2* and the Online help for information about importing devices from third party NMS.

Network Management Integration Data Bundle (NMIDB) 1.0.089 is shipped with LMS 3.1.

You can download the latest adapters for third-party network management applications and the Network Management Integration Data Bundle (NMIDB) from the following locations:

- Latest Adapters at:

<http://www.cisco.com/kobayashi/sw-center/cw2000/cmc3rd.shtml>

To access the above page, you must be a registered user of Cisco.com.

- NMIDB at:

<http://download-sj.cisco.com/cisco/netmgmt/ciscoview/5.0/packages/nmidb.X.zip>

(On Internet Explorer and Firefox browsers)

Where X is the version of NMIDB.

Supported Devices

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

Registered Cisco.com users can access the most current Device Package Updates, and download the latest device updates for CV, CM, DFM and RME from the following location:

- For CiscoView at:
<http://www.cisco.com/cgi-bin/Software/CiscoView/cvplanner.cgi>
- For Campus at:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-campus>
- For DFM at:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>
- For RME at:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme>

To see the list of installed application's device packages, select **Common Services > Software Center** and then select the required application name on the CiscoWorks home page.

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

- Supported Devices Tables of RME, CM, CV, and DFM (LMS 3.1)
This document is available on Cisco.com at the following URLs:
http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html
http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products_device_support_tables_list.html
- User Guide for CiscoView 6.1.8
CiscoView manages and configures different types of Cisco devices. You can refer this document for information on supported devices. This document is available on Cisco.com at this URL:
http://www.cisco.com/en/US/products/sw/cscowork/ps4565/products_user_guide_list.html



CHAPTER 2

Prerequisites

This chapter describes the factors that you must consider before installing CiscoWorks LAN Management Solution 3.1 on both Windows and Solaris systems.

This chapter contains:

- [System and Browser Requirements for Server and Client](#)
- [Terminal Server Support for Windows 2003 Server](#)
- [Solaris Patches](#)
- [LAN Management Solution Port Usage](#)
- [Required Device Credentials for LMS Applications](#)

System and Browser Requirements for Server and Client

Before you begin to install LAN Management Solution 3.1 applications, you must check if your system meets the recommended prerequisites.

The recommended LAN Management Solution 3.1 server and client requirements on both Operating Systems are based on the license that you use on a single server or multi-server setup.

Disk Space requirements without HUM

The disk space required to install all LMS applications with HUM Add-on, on both Solaris and Windows is:

- 25 GB free space for LMS applications and data, in the CiscoWorks installation directory— For LMS 100 (Windows) and LMS 300 device license types.
- 35 GB free space for LMS applications and data, in the CiscoWorks installation directory— For LMS 1,500, LMS 5,000, and LMS 10,000 device license types.

Disk Space requirements with HUM

The disk space required to install all LMS applications with HUM Add-on, on both Solaris and Windows is:

- 45 GB free space for LMS and HUM applications and data, in the CiscoWorks installation directory— For LMS 100 (Windows) and LMS 300 device license types and for HUM 50 and HUM 300 device license types
- 85 GB free space for LMS and HUM applications and data, in the CiscoWorks installation directory— For LMS 1,500, LMS 5,000, and LMS 10,000 device license types and for HUM 1,000 device license types

Disk Space requirement with HUM on a Standalone Server

The disk space required to install HUM Add-on in Standalone mode, on both Solaris and Windows is:

- 20 GB free space for HUM applications and data, in the CiscoWorks installation directory— For HUM 50 and HUM 300 device license types.
- 50 GB free space for HUM applications and data, in the CiscoWorks installation directory— For HUM 1,000 device license types.

The hardware requirements vary based on the type of device restricted license you use.

- [Table 2-1](#) lists the server hardware requirements for installing the LAN Management Solution 3.1 components on Solaris systems.
- [Table 2-3](#) lists the server hardware requirements for installing the LAN Management Solution 3.1 components on Windows systems.
- [Table 2-5](#) lists the client system requirements for all platforms.

If you are running additional Cisco or third-party applications on the servers, the requirements might be higher.



Note

LMS 3.1 is not supported on Windows 2000 and Solaris 8 servers.

This section contains the following:

- [Operating System Requirements](#)
- [Server Requirements on Solaris Systems](#)
- [Server Requirements on Windows Systems](#)
- [System Requirements on Client Servers](#)

Operating System Requirements

LMS 3.1 runs on systems with following Operating Systems:

- Solaris Systems
 - Solaris 9
 - Solaris 10

LMS 3.1 is installed on global zone of Solaris 10 Operating System by default.

Installation of LMS 3.1 is supported on whole-root non-global zone. For details, see [Support for Zone-based Virtualization in Solaris 10](#).

LMS 3.1 also supports Logical domains (LDoms) and ZFS file system.

See [Solaris Patches](#) for more information on Solaris patches to be installed on these Operating Systems.

- Windows Systems
 - Windows Server 2003 Standard Edition
 - Windows Server 2003 Enterprise Edition
 - Windows Server 2003 R2 Standard Edition
 - Windows Server 2003 R2 Enterprise Edition
 - Windows Server 2003 Standard Edition with Service Pack 1 and 2
 - Windows Server 2003 Enterprise Edition with Service Pack 1 and 2
 - Windows Server 2003 R2 Standard Edition with Service Pack 1 and 2
 - Windows Server 2003 R2 Enterprise Edition with Service Pack 1 and 2

Both 32 bit and 64 bit Operating Systems are supported on the above versions

- Virtualization Systems
 - VMware ESX server 3.0.1
 - VMware ESX Server 3.5.0

Server Requirements on Solaris Systems

Table 2-1 lists the server requirements for installing the LAN Management Solution 3.1 components on Solaris systems without HUM.

Table 2-2 lists the server requirements for installing the LAN Management Solution 3.1 components on Solaris systems with HUM.

Table 2-1 Recommended Server Hardware Requirements on Solaris Systems without HUM

Component	Recommended Server System Requirement
LMS 300	<ul style="list-style-type: none"> UltraSPARC CPU with 2 GB RAM memory requirement and 4 GB swap space on Solaris 9. UltraSPARC CPU with 4 GB RAM memory requirement and 8 GB swap space on Solaris 10. <p>The memory requirements for LMS 300 device license type vary on Solaris 9 and Solaris 10 systems.</p>
LMS 1,500	UltraSPARC 2 CPUs with 4 GB RAM memory requirement and 8 GB swap space.
LMS 5,000 <ul style="list-style-type: none"> Standalone server: <ul style="list-style-type: none"> DFM, IPM, RME and Campus will support up to 5,000 devices. Solution server: <ul style="list-style-type: none"> Maximum of 5,000 devices in each application. <p>To manage 5,000 devices for all applications including DFM and HUM, you must setup:</p> <ul style="list-style-type: none"> DFM on a Standalone server (with only CS and DFM installed) HUM on a Standalone server (with only CS and HUM installed), which manages 1000 devices All other CiscoWorks applications on another server 	<ul style="list-style-type: none"> Standalone server: <ul style="list-style-type: none"> UltraSPARC 2 CPUs with 4 GB RAM memory requirement and 8 GB swap space. Solution server: <ul style="list-style-type: none"> UltraSPARC 4 CPUs with 8 GB RAM memory requirement and 16 GB swap space.
LMS 10,000 <ul style="list-style-type: none"> Standalone server: <ul style="list-style-type: none"> RME will support up to 10,000 devices. DFM, IPM and Campus will support up to 5,000 devices. <p>More than one server must be used to manage up to 10,000 devices.</p>	<ul style="list-style-type: none"> Standalone server: <ul style="list-style-type: none"> UltraSPARC 2 CPUs with 4 GB RAM memory requirement and 8 GB swap space.

[Table 2-2](#) lists the server requirements for installing the LAN Management Solution 3.1 components on Solaris systems with HUM.

Table 2-2 Recommended Server Hardware Requirements on Solaris Systems with HUM

Component	Recommended Server System Requirement
LMS Bundle Hardware Configuration	
HUM 50— 50 devices + LMS 300	<ul style="list-style-type: none"> One UltraSPARC CPU with 2 GB RAM memory and 4 GB swap space on Solaris 9 One UltraSPARC CPU with 4 GB RAM memory and 8 GB swap space on Solaris 10
HUM 300—300 devices + LMS 1500	Two UltraSPARC CPUs with 4 GB RAM memory and 8 GB swap space for Solaris 9 and 10.
Standalone Hardware Configuration	
HUM 50— 50 devices	<ul style="list-style-type: none"> One UltraSPARC CPU with 2 GB RAM memory and 4 GB swap space on Solaris 9 One UltraSPARC CPU with 4 GB RAM memory and 8 GB swap space on Solaris 10
HUM 300—300 devices	Two UltraSPARC CPUs with 4 GB RAM memory and 8 GB swap space for Solaris 9 and 10.
HUM 1000— Upto 1000 devices	Four UltraSPARC CPUs with 8 GB RAM memory and 16 GB swap space for Solaris 9 and 10.

The following are the supported processors on a Solaris system:

- UltraSPARC III (280R, 480R)
- UltraSPARC IIIi processor (V240, V250, V440)
- UltraSPARC IV processor (V490, V890)
- UltraSPARC IV+ processor (V490, V890)
- UltraSPARC T1 processor (Sun Fire T1000 Server, Sun Fire T2000 Server)
- UltraSPARC T2 processor (Sun SPARC Enterprise T5120 Server)

See [Solaris Patches, page 2-10](#) for information on required and recommended server patches on Solaris systems.



Note

LMS 100 devices restricted license type is not supported on Solaris systems.

Server Requirements on Windows Systems

[Table 2-3](#) lists the server requirements for installing the LAN Management Solution 3.1 components on Windows systems without HUM.

[Table 2-4](#) lists the server requirements for installing the LAN Management Solution 3.1 components on Windows systems with HUM.

For a list of Windows HotFix patches, see the [Frequently Asked Questions](#).

Table 2-3 *Recommended Server Hardware Requirements on Windows Systems without HUM*

Component	Recommended Server System Requirement
LMS 100	1 CPU with 2 GB RAM memory requirement with a swap space of 4 GB.
LMS 300	1 CPU with 2 GB RAM memory requirement with a swap space of 4 GB.
LMS 1,500	2 CPUs with 4 GB RAM memory requirement with a swap space of 8 GB.
LMS 5,000 <ul style="list-style-type: none"> Standalone server: <ul style="list-style-type: none"> DFM, IPM, RME and Campus will support up to 5,000 devices. Solution server: <ul style="list-style-type: none"> Maximum of 5,000 devices in each application. <p>To manage 5,000 devices for all applications including DFM and HUM, you must setup:</p> <ul style="list-style-type: none"> DFM on a Standalone server (with only CS and DFM installed) HUM on a Standalone server (with only CS and HUM installed), which manages 1000 devices All other CiscoWorks applications on another server 	<ul style="list-style-type: none"> Standalone server: <ul style="list-style-type: none"> 2 CPUs with 4 GB RAM memory requirement and 8 GB swap space. Solution server: <ul style="list-style-type: none"> 4 CPUs with 8 GB RAM memory requirement and 16 GB swap space.
LMS 10,000 <ul style="list-style-type: none"> Standalone server: <ul style="list-style-type: none"> RME will support up to 10,000 devices. DFM, IPM and Campus will support up to 5,000 devices. <p>More than one server must be used to manage up to 10,000 devices.</p>	<ul style="list-style-type: none"> Standalone server: <ul style="list-style-type: none"> 2 CPUs with 4 GB RAM memory requirement and 8 GB swap space. Solution server: <ul style="list-style-type: none"> 4 CPUs with 8 GB RAM memory requirement and 16 GB swap space.

Table 2-4 lists the server requirements for installing the LAN Management Solution 3.1 components on Windows systems with HUM.

Table 2-4 Recommended Server Hardware Requirements on Windows Systems with HUM

Component	Recommended Server System Requirement
LMS Bundle Hardware Configuration	
HUM 50— 50 devices + LMS 300	One CPU with 2 GB RAM memory and 4 GB swap space running Windows 2003 Server.
HUM 300—300 devices + LMS 1500	One CPU with 2 GB RAM memory and 4 GB swap space running Windows 2003 Server.
Standalone Hardware Configuration	
HUM 50— 50 devices	One CPU with 2 GB RAM memory and 4 GB swap space.
HUM 300—300 devices	One CPU with 2 GB RAM memory and 4 GB swap space.
HUM 1000—Upto 1000 devices	Two CPUs with 4 GB RAM memory and 8 GB swap space.

The following are the supported processors on a Windows system:

For Intel:

- Intel® Xeon® processor (Dual Core)
- Intel® Core™ Duo processor T2600 - T2300
- Intel® Pentium® processor Extreme Edition 965 (Dual Core)
- Intel® Pentium® D processor 960 (Dual Core)
- Intel® Pentium® 4 processor with Hyper-Threading Technology
- Quad-Core Intel Xeon processor 5400 series
- Quad-Core Intel Xeon processor 5300 series
- Quad-Core Intel Xeon processor 7300 series

For AMD:

- Dual-Core AMD Opteron Processor
- AMD Opteron Processor
- AMD Athlon 64 FX Processor
- AMD Athlon™ 64 X2 Dual-Core

VMWare Optimized hardware:

- Intel-VT processors
 - Intel® vPro™ processor technology
 - Intel® Xeon® processor 5000 sequence
 - Intel Xeon processor 7000 sequence

- Intel Xeon processor 3000 sequence
- Intel® Itanium® Processor 9000 sequence
- AMD-V

System Requirements on Client Servers

[Table 2-5](#) lists the client system requirements for all platforms.

Table 2-5 Recommended Client Hardware and Software Requirements

Component	Recommended Client System Requirement
Operating System	<p>The hardware recommended for the client systems are:</p> <ul style="list-style-type: none"> • Windows systems: PC-compatible system with single CPU 2.4 GHz or equivalent processor running: <ul style="list-style-type: none"> – Windows Server 2003 Standard and Enterprise Editions with Service Pack 1 and 2 – Windows Server 2003 R2 Standard and Enterprise Editions with Service Pack 1 and 2 <p>Both 32 bit and 64 bit Operating Systems are supported on the above versions</p> <ul style="list-style-type: none"> – Windows XP Professional with Service Pack 2, Service Pack 3 – Windows Vista Business Edition with Service Pack 1 <p>LAN Management Solution 3.1 supports only the US English and Japanese versions of these operating systems. Set the default locale to US-English for the US-English version and Japanese for the Japanese version.</p> <ul style="list-style-type: none"> • Solaris systems: Sun UltraSPARC processor with Solaris 9 and Solaris 10 with latest patches and upgrades. See Solaris Patches for information on required and recommended server patches on Solaris systems.
Memory requirements	<p>512 MB minimum RAM</p> <p>Either of the following:</p> <ul style="list-style-type: none"> • For Solaris: 1 GB swap space • For Windows: 1 GB virtual memory <p>We recommend that you set virtual memory and swap space to twice the size of RAM.</p>
JVM Requirements	Java Plug-in version 1.6.0_05.
Browser Requirements	<ul style="list-style-type: none"> • Internet Explorer 6.0 Service Pack 1, Service Pack 2 • Internet Explorer 7.0 • Firefox 2.0 <p>Note Solaris systems support only Firefox 2.0 browsers.</p>

Terminal Server Support for Windows 2003 Server

You can install Common Services and LMS applications on a system with Terminal Services enabled in Remote Administration mode. However, you cannot install Common Services on a system with Terminal Services enabled in Application mode.

If you have enabled Terminal Server in Application mode, you should disable the Terminal Server, reboot the system, and start the installation again.

Table 2-6 summarizes the Terminal Services features in Windows 2003 Server.

Table 2-6 *Terminal Services on Windows 2003 Server*

Windows 2003 Server	Features
Terminal Server	Remote access and virtual system. Each client has its own virtual OS environment.
Remote Desktop Administration	Remote access only. All clients use the same (and the only) OS.

Enabling and Disabling Terminal Services on Windows 2003 Server

To enable/ disable Terminal Server, go to **Manage Your Server > Add or Remove a Role > Terminal Server**.

To enable/ disable Remote Desktop Administration, go to **Control Panel > System > Remote**.

Enabling and Disabling FIPS on Windows 2003 Server

Sometimes, Federal Information Processing Standard (FIPS) compliant encryption algorithms are enabled for Group security policy on Windows server.

When the FIPS compliance is turned on, the SSL authentication may fail on CiscoWorks Server. You should disable the FIPS compliance for the CiscoWorks to work properly.

To enable/disable FIPS on Windows 2003 server:

-
- Step 1** Go to **Start > Settings > Control Panel > Administrative tools > Local Security Policy**.
The Local Security Policy window appears.
 - Step 2** Click **Local Policies > Security Options**.
 - Step 3** Select **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
 - Step 4** Right-click the selected policy and click **Properties**.
 - Step 5** Select **Enabled** or **Disabled** to enable or disable FIPS compliant algorithms.
 - Step 6** Click **Apply**.
You must reboot the server for the changes to take effect.
-

Solaris Patches

LMS 3.1 is installed on global zone of Solaris 10 Operating System by default. Installation of LMS 3.1 in whole-root non-global zone in Solaris 10 is supported.

The Solaris system requires the following patches to be installed on the server:

- [Required and Recommended Solaris Patches](#)
- [Cluster Patches](#)

Required and Recommended Solaris Patches

[Table 2-7](#) lists the required and recommended patches for Solaris 9.

The required patches are mandatory for all LMS features to function properly. Some of the LMS features may not work if the mandatory patches are not installed on your system.

The recommended patches are optional.

For example, the required patch for LMS is 112963-20. If you install the patches 112963-21 through 112963-24, the following error message appears and installation may fail:

```
INFO: Patch 112963-20 is superceded by a newer patch.
```

To complete the installation of LMS applications, you must downgrade to patch 112963-20 on Solaris 9 system.

For more information, see <http://www.sun.com>.

Table 2-7 *Solaris Patches*

Operating System	Required Server Patches	Required Client Patches	Recommended Server Patches	Recommended Client Patches
Solaris 9	114224-01 113580-01 112839-04 112233-12 114006-01 118558-39 112874-31 113225-09 111722-05	112771-14 112661-06 113244-05	113326-01 112998-03 113713-14 112964-07 113575-05 112970-07	112808-06
Solaris 10	<ul style="list-style-type: none"> • Required Server Patch is 122032-05. • Minimum system level must be 11/06 release or higher. <p>To find out the current operating system level, enter the following command:</p> <pre># more /etc/release</pre> <p>For example, the system displays the following information:</p> <pre>Solaris 10 11/06 s10s_u2wos_09a SPARC Copyright 2006 Sun Microsystems, Inc. All Rights Reserved. Use is subject to license terms. Assembled 11 November 2006</pre>			

Use `showrev -p` command to verify that these patches have been applied.


Note

LMS was tested only with these patches. Later versions of these patches have not been tested since they were not released when LMS was tested.

The table below lists the messages that appear during installation if you do not have the recommended and required Solaris patches on the system.

If you do not have...	Message
Required Server patches	<p>Warning message appears with a prompt to continue or quit the installation.</p> <pre>This system does not have the following required Server patches Installation can proceed without the required Server patches.However, you must install the required patches listed above before running CiscoWorks. Do you want to continue the installation? (y/n) [y]:</pre>
Required Client patches	<p>Warning message appears with a prompt to continue or quit the installation.</p> <pre>This system does not have the following required Client patches. These patches are required if only this system is used as a CiscoWorks client.</pre>
Recommended Server patches	<p>Warning message appears with a prompt to continue or quit the installation.</p> <pre>This system does not have the following recommended Server patches.</pre>
Recommended Client patches	<p>Warning message appears with a prompt to continue or quit the installation.</p> <pre>This system does not have the following recommended Client patches. These patches are recommended if only this system is used as a CiscoWorks client.</pre>

We recommend you download and install the latest required and recommended patches from <http://www.sun.com> before you run LMS applications.

Cluster Patches

You should also install the cluster patches recommended by Sun Microsystems on both Solaris 9 and Solaris 10 servers.

You can download the cluster patches from <http://www.sun.com> . See the same website for the installation instructions of Cluster patches.

The minimum recommended cluster patch levels on Solaris Systems are:

- Solaris 9 — Cluster patches released on Dec/11/06.
- Solaris 10 — Cluster patches released on Apr/17/07.

If you have not installed the cluster patches on Solaris 9 system, the following warning messages appear to ensure you install the Cluster Patches required for Solaris 9:

```
WARNING: Ensure that you have installed the recommended Solaris 9 cluster patches released
on Dec/11/06, in this server.
WARNING: If these cluster patches are not installed, please download and install them
from http://www.sun.com/.
WARNING: Otherwise, some features of the CiscoWorks applications will not function
properly.
Do you want to continue the installation ? (y/n) [y]:
```

If you have not installed the cluster patches on Solaris 10 system, the following warning messages appear to ensure you install the Cluster Patches required for Solaris 10:

```
WARNING: Ensure that you have installed the recommended Solaris 10 cluster patches
released on Apr/17/07, in this server.
WARNING: If these cluster patches are not installed, please download and install them from
http://www.sun.com/.
WARNING: Otherwise, some features of the CiscoWorks applications will not function
properly.
Do you want to continue the installation ? (y/n) [y]:
```


LAN Management Solution Port Usage

Table 2-8 lists the ports used by the various CiscoWorks components

Table 2-8 LAN Management Solution Port Usage

Protocol	Port Number	Service Name	Applications	Direction (of Establishment) of Connection
TCP	49	TACACS+ and ACS	CiscoWorks Common Services, RME, Campus, DFM and IPM	Server to ACS
TCP	25	Simple Mail Transfer Protocol (SMTP)	CiscoWorks Common Services (PSU), RME	Server to SMTP Server
TCP	22	Secure Shell (SSH)	CiscoWorks Common Services, Campus, and RME	Server to Device
TCP	23	Telnet	CiscoWorks Common Services, Campus, and RME	Server to Device
UDP	69	Trivial File Transfer Protocol (TFTP)	CiscoWorks Common Services and RME	Server to Device Device to Server
UDP	161	Simple Network Management Protocol (SNMP)	CiscoWorks Common Services, CiscoView, RME, Campus, DFM, IPM and HUM	Server to Device Device to Server
TCP	514	Remote Copy Protocol	CiscoWorks Common Services	Server to Device
UDP	162	SNMP Traps (Standard Port)	Campus and DFM	Device to Server
UDP	514	Syslog	CiscoWorks Common Services and RME	Device to Server
UDP	1431	Trap Listener to MAC Notification Traps	Campus	Device to Server
UDP	9000	DFM trap receiving (if port 162 is occupied)	DFM	Device to Server
UDP	16236	UT Host acquisition	Campus	End host to Server
TCP	443	CiscoWorks HTTP server in SSL mode	CiscoWorks Common Services	Client to Server Server Internal
TCP	1741	CiscoWorks HTTP Protocol	CiscoWorks Common Services, CiscoView, Campus, RME, DFM and IPM	Client to Server
UDP	42342	OSAGENT	CiscoWorks Common Services	Client to Server (for ANIServer)
TCP	42352	ESS HTTP (Alternate port is 44352/tcp)	CiscoWorks Common Services	Client to Server
TCP	8898	Log Server	DFM	Server Internal

Table 2-8 LAN Management Solution Port Usage (continued)

Protocol	Port Number	Service Name	Applications	Direction (of Establishment) of Connection
TCP	9002	DynamID authentication (DFM Broker)	DFM	Server Internal
TCP	9007	Tomcat shutdown	CiscoWorks Common Services	Server Internal
TCP	9009	Ajp13 connector used by Tomcat	CiscoWorks Common Services	Server Internal
UDP	9020	DFM Trap Receiving	DFM	Server Internal
TCP	10002	OpsXML message bus, OpsXMLRuntime	CiscoWorks Assistant	Server Internal
UDP	14004	Lock port for ANI Server singlet on check	Campus	Server Internal
TCP	15000	Log server	DFM	Server Internal
TCP	40050-40070	CSTM ports used by CS applications, such as OGS, Device and Credential Repository (DCR)	CiscoWorks Common Services	Server Internal
TCP	40401	LicenseServer	CiscoWorks Common Services	Server Internal
TCP	42340	CiscoWorks Daemon Manager - Tool for Server Processes	CiscoWorks Common Services	Server Internal
TCP	42344	ANI HTTP Server	CiscoWorks Common Services	Server Internal
UDP	42350	Event Services Software (ESS) (Alternate port is 44350/udp)	CiscoWorks Common Services	Server Internal
TCP	42351	Event Services Software (ESS) Listening (Alternate port is 44351/tcp)	CiscoWorks Common Services	Server Internal
TCP	42353	ESS Routing (Alternate port is 44352/tcp)	CiscoWorks Common Services	Server Internal
TCP	43441	CMF Database	CiscoWorks Common Services	Server Internal
TCP	43455	RME Database	RME	Server Internal
TCP	43443	ANIDbEngine	Campus	Server Internal
TCP	43445	Fault History Database	DFM	Server Internal
TCP	43446	Inventory Service Database	DFM	Server Internal

Table 2-8 *LAN Management Solution Port Usage (continued)*

Protocol	Port Number	Service Name	Applications	Direction (of Establishment) of Connection
TCP	43447	Event Promulgation Module Database	DFM	Server Internal
TCP	44400- 44420	CSTM Port for DFM, HUM	DFM, HUM	Server Internal
TCP	47000- 47040	CSTM Port for RME	RME	Server Internal
TCP	49154	UPMDbEngine	HUM	Server Internal
TCP	49155	OpsxmlDbEngine, JDBC / ODBC	CiscoWorks Assistant	Server Internal
TCP	49157	IPM Database	IPM	Server Internal
TCP	50001	SOAPMonitor	RME	Server Internal
TCP	55000- 55020	CSTM Port for Campus Manager	Campus	Server Internal

Required Device Credentials for LMS Applications

You must configure several important device credentials correctly on every Cisco device that will be managed and monitored through LMS. You must also enter the correct device credentials in the Device and Credential Repository (**Common Services > Device and Credentials > Device Management**).

Table 2-9 lists all the applications and the device credentials required for proper functioning of the applications.

Table 2-9 Applications and Device Credentials

Application	Telnet/SSH Password	Enable Password	SNMP Read Only	SNMP Read / Write
Common Services	Not required	Not required	Required	Required
Campus Manager	Not required	Not required	Required	Required
CiscoView	Not required	Not required	Required	Required
Device Fault Manager	Not required	Not required	Required	Not required
Internetwork Performance Monitor	Not required	Not required	Required	Required
Health and Utilization Monitor	Not required	Not required	Required	Not required
Resource Manager Essentials				
Inventory	Not required	Not required	Required	Not required
Configuration Management (Telnet)	Required	Required	Required	Not required
Configuration Management ¹ (TFTP) ²	Not required	Not required	Required	Required
NetConfig	Required	Required	Required	Required
Config Editor	Required	Required	Required	Required
NetShow	Required	Required	Required	Not required
Software Management	Required ³	Required ³	Required	Required

1. Configuration download also uses TFTP. Hence, SNMP Read/Write credentials are required.

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

3. Required in the case of a few devices like PIX devices, Cisco 2950 series switches.



CHAPTER 3

Preparing to Install CiscoWorks LAN Management Solution 3.1

This chapter lists the necessary information that prepares you to perform an installation of CiscoWorks LMS 3.1 on both Windows and Solaris systems.

This chapter contains:

- [Terms and Definitions Used in LMS Installation Framework](#)
- [Before You Begin Installation](#)
- [License Information](#)
- [Application Scaling Numbers](#)
- [Licensing Your Product](#)

Terms and Definitions Used in LMS Installation Framework

This section captures the terms and definitions that are used by LMS applications at the time of installation.

See [Licensing Your Product](#) to understand the licensing terminologies.

LMS Application Database Password

In LMS 3.1, the LMS Application Database Password is requested during Custom installation. This database password is used internally by all the LMS applications to communicate with the respective application's database. This password is also used while restoring or troubleshooting the database.

Use a minimum of five characters and a maximum of 15 characters. Do not start the password with a number and do not insert spaces between characters.



Note

While installing applications in Custom mode alone you will be prompted to enter the LMS Application database password. In the Typical mode, this password is randomly generated.

While installing, you will come across these terms:

- CiscoWorks Admin Password

An administrative password used while logging into the CiscoWorks server as administrator. Use a minimum of five characters.

Ensure that you have noted down the password.

You are prompted to enter this password in both Typical and Custom modes of installation.

- System Identity Account Password

Password that is used in a multi-server environment.

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

You must configure all the CiscoWorks servers that are part of your multi-server setup with the same system identity account password.

While entering the System Identity Account Passwords, use a minimum of five characters.

You are prompted to enter this password in both Typical and Custom modes of installation.

- CiscoWorks Guest Password

This is used while logging into the CiscoWorks server as a guest user. Use a minimum of five characters.

You are prompted to enter this password in the Custom mode of installation. In the Typical mode, this password is randomly generated.

- Self Signed Certificate

CiscoWorks allows you to create security certificates to enable SSL communication between your client browser and management server.

Self Signed Certificates are valid for five years from the date of creation. When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed CiscoWorks.

For more information on Self Signed Certificates, see [User Inputs for Custom Installation](#).

In the Typical mode, this certificate is automatically generated.

For more information on passwords, see [Password Rules for New Installation](#)

- SMTP Server

System-wide name of the SMTP server used by CiscoWorks applications to deliver reports. The default server name is localhost.

You are prompted to enter this server detail only in the Custom mode of installation. In the Typical mode, after the installation you can configure SMTP by selecting **Common Services > Server > Admin > System Preferences** from the CiscoWorks home page.

- Cisco.com

Cisco.com user ID and password. This information is used while performing tasks such as downloading software images, downloading device packages, etc.

You are prompted to enter these credentials only while installing the CiscoWorks Integration Utility.

You can also change the System Identity Account password, Guest password, and Cisco.com credentials using the Common Services User Interface (**Common Services > Server > Security**).

Before You Begin Installation

This section contains the following important information that you should read before you begin installation:

- [Installation Notes](#)
- [Installation Notes \(For Solaris Only\)](#), page 3-4
- [Installation Notes \(For Windows Only\)](#), page 3-5

Installation Notes

Before you begin the installation, read the following notes:

- Close all open or active programs. Do not run other programs during the installation process.
- By default, SSL is not enabled on CiscoWorks Server.
- While launching CiscoWorks, network inconsistencies might cause installation errors if you are installing from a remote mount point.
- If your CiscoWorks Server is integrated with any Network Management System (NMS) in your network using the Integration Utility, you must perform the integration whenever you enable or disable SSL in the CiscoWorks Server. You must do this to update the application registration in the NMS.

For help with NMS integration, see the *User Guide for CiscoWorks Integration Utility 1.7*. You can find this document on Cisco.com, in both HTML and PDF form.

http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html

- Disable any popup blocker utility that is installed on your client system before launching CiscoWorks.
- CiscoWorks applications are installed in the default directories:
 - On Solaris: `/opt/CSCOpX`
 - On Windows: `SystemDrive:\Program Files\CSCOpX`

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

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

The destination folder should not contain the following special characters:

- On Solaris:


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


```
! @ # $ % ^ & * ( ) + | } { " [ ] ; ' / ? < > , . ` =
```
- If errors occur during installation, check the installation log file:
 - On Solaris, check the installation log file
`/var/tmp/Ciscoworks_install_YYYYMMDD_hhmmss.log` for LMS 3.1 installation
 Where *YYYYMMDD* denotes the year, month and date of installation and *hhmmss* denotes the hours, minutes and seconds of installation.
 For example:
`/var/tmp/Ciscoworks_install_20060721_182205.log`

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

For example, for LMS 3.1, the installation log file is:

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

For example:

C:\Ciscoworks_install_20060721_182205.log

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

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



Note

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

- If HP OpenView is running on your system, installation will take more time. Disable HP OpenView to run a faster installation.
- To ensure that you have the latest device support and bug fixes for Resource Manager Essentials, Campus Manager, Device Fault Manager, and CiscoView you must install the latest Service Packs.

For download locations, see the [Supported Devices](#).

Installation Notes (For Solaris Only)

- On Solaris, if you select an installation directory other than the default, the /opt/CSCOpX directory is created as a link to the directory you selected.



Warning

If you remove this link after installation, the product will malfunction.

- We recommend that you run the installation from a local CD or a local hard drive to avoid errors that may result from the network being slow or busy.

If you want to install from a local hard drive, you must copy the contents from the CD to the local hard drive. Ensure that you copy the entire contents from the CD to the hard drive.

You must preserve the timestamp when you copy the contents from the CD to the hard drive.

To preserve all the attributes including timestamp:

- Change the present working directory to the directory to which the CD is mounted using the command:

```
cd /cdrom/cdrom0
```

where **cdrom/cdrom0** is the directory to which the CD is mounted.

- Create a directory where you want to copy the contents of the disk by entering:

```
mkdir /opt/copydisk
```

Make sure that this directory has enough space to hold the entire contents of the disk.

- Enter:

```
tar cpf - . | (cd /opt/copydisk && tar -xpf -)
```

This command preserves all attributes including the timestamp.

Installation Notes (For Windows Only)

- You can install LMS 3.1 applications on a system with Terminal Services enabled in Remote Administration mode. However, installation of LMS 3.1 applications on a system with Terminal Services enabled in Application mode is not supported.

If you have enabled Terminal Server in Application mode, disable the Terminal Server, reboot the system, and start the installation again. See [Terminal Server Support for Windows 2003 Server](#).

- If Internet Information Services (IIS) is detected on your system and if you have continued the installation with IIS services, you cannot use the port number 443 for HTTPS. Instead, you must use the port numbers ranging from 1026 to 65535 for HTTPS to avoid this conflict.
- If you are running any virus scanner while installing LMS applications, the installation might take longer to complete.

We recommend that you disable the virus scan software on your system. You can restart it after all installations are completed.

- Check the Primary and Active regional settings before installation. They have to be set either as US English or Japanese. Other options are not supported by LMS 3.1.

You can set the Active regional settings in **Control Panel > Regional and Language Options > Regional Options**.

- You must restart your system after you install LMS 3.1 to avoid any system instability on a Windows OS.

License Information

The licenses in LMS 3.1 are device based for all applications. For 10000 device licenses, applying a single serial license key to more than one server is supported. Please see the [SUPPLEMENTAL LICENSE AGREEMENT](#) section for more details.

For Internetwork Performance Monitor (IPM) alone, besides the number of devices, the number of collectors you create depends on the license.

Available Licenses (SKU) in LMS 3.1	Permitted number of Devices and Collectors in LMS 3.1 (RME, Campus, DFM and IPM)
CWLMS-3.1-100-K9	100 devices and 300 collectors
CWLMS-3.1-300-K9	300 devices and 1,000 collectors
CWLMS-3.1-1.5K-K9	1,500 devices and 1,500 collectors
CWLMS-3.1-5K-K9	5,000 devices and 5,000 collectors
CWLMS-3.1-10K-K9	10,000 devices and 5,000 collectors

**Note**

The LMS 100 devices license is supported only on Windows systems. This is not supported on Solaris systems.

Add-on Component(s) to LMS

Separate license is required to install CiscoWorks Health and Utilization Monitor (HUM) 1.1, add-on component to LMS 3.1. Following are the SKUs available for HUM 1.1:

Available Licenses (SKU) in HUM 1.1	Permitted number of Devices in HUM 1.1
CWHUM-1.1-S-K9	50 devices restricted license
CWHUM-1.1-M-K9	300 devices restricted license
CWHUM-1.1-L-K9	1000 devices restricted license
Upgrade Licenses (SKU) in HUM 1.1	
CWHUM-1.1-S2M-K9	Upgrade from 50 devices to 300 devices
CWHUM-1.1-S2L-K9	Upgrade from 50 devices to 1000 devices
CWHUM-1.1-M2L-K9	Upgrade from 300 devices to 1000 devices

If you have LMS 3.0 license with Software Application Support (SAS) contracts, you can order LMS 3.1 using the Product Upgrade Tool at www.cisco.com/upgrade. The SKUs that need to be used while ordering are:.

Licenses (SKU) to upgrade from LMS 3.0	Permitted number of Devices
CWLMS-3.1-100SRK9	LMS 3.0 100 Device Restricted Upgrade to LMS 3.1
CWLMS-3.1-300-SRK9	LMS 3.0 300 Device Restricted Upgrade to LMS 3.1
CWLMS-3.1-1.5KSRK9	LMS 3.0 1500 Device Restricted Upgrade to LMS 3.1
CWLMS-3.1-5K-SR-K9	LMS 3.0 5000 Device Restricted Upgrade to LMS 3.1
CWLMS-3.1-10K-SRK9	LMS 3.0 10000 Device Restricted Upgrade to LMS 3.1

If you have LMS 3.0 license without Software Application Support (SAS) contracts, you can order LMS 3.1 from www.cisco.com. The SKUs that need to be used while ordering are:.

Licenses (SKU) to upgrade from LMS 3.0	Permitted number of Devices
CWLMS-3.1-100MR-K9	LMS 3.0 100 Device Restricted Upgrade to LMS 3.1
CWLMS-3.1-300MR-K9	LMS 3.0 300 Device Restricted Upgrade to LMS 3.1
CWLMS-3.1-1.5KMRK9	LMS 3.0 1500 Device Restricted Upgrade to LMS 3.1
CWLMS-3.1-5KMR-K9	LMS 3.0 5000 Device Restricted Upgrade to LMS 3.1
CWLMS-3.1-10KMR-K9	LMS 3.0 10000 Device Restricted Upgrade to LMS 3.1

To upgrade from LMS 2.5.x, LMS 2.6, you can order LMS 3.1 through Cisco Sales channels. The SKUs that need to be used while ordering are:

Licenses (SKU) to upgrade from LMS, LMS 2.6	Permitted number of Devices
CWLMS-3.1-300UPK9	LMS 3.1 300 Device Restricted Upgrade for LMS 2.5.x, 2.6
CWLMS-3.1-1.5KUPK9	LMS 3.1 1500 Device Restricted Upgrade for LMS 2.5.x, 2.6

Licenses (SKU) to upgrade from LMS, LMS 2.6	Permitted number of Devices
CWLMS-3.1-5KUPK9	LMS 3.1 5000 Device Restricted Upgrade for LMS 2.5.x, 2.6
CWLMS-3.1-10KUPK9	LMS 3.1 10000 Device Restricted Upgrade for LMS 2.5.x, 2.6

See [Application Scaling Numbers](#) for further deployment related information.

Application Scaling Numbers

This section presents information on the specific scaling numbers for each of the CiscoWorks LMS applications in both Standalone server as well as in a Solution server:

- [Standalone Server](#)
- [Solution Server](#)
- [Concurrent Users Supported](#)

Standalone Server

The application scaling numbers on a Standalone Server are:

- Common Services Device and Credential Repository (DCR)—Maximum of 50,000 devices and 100 user-defined groups.
- Resource Manager Essentials (RME)—10,000 devices and 100 user-defined groups.
- Campus Manager—5,000 devices, 250,000 end hosts and IP Phones, and 100 user-defined groups.
Campus Manager Data Collection discovers and tracks a maximum of 150,000 Switch Ports.
- Device Fault Manager (DFM)—5,000 devices with a maximum of 80,000 ports or interfaces of which upto 15 percent can be in managed state. It also supports 100 user-defined groups.
- Internetwork Performance Monitor (IPM)—5,000 devices with a maximum of 5,000 collectors.
- Health and Utilization Monitor (HUM)
 - 50 devices with a maximum of 30,000 MIB objects
 - 300 devices with a maximum of 30,000 MIB objects
 - 1000 devices with a maximum of 100,000 MIB objects

Solution Server

LMS 3.1 now supports up to 5,000 devices for all applications that are installed in a single Solution server, except DFM and HUM. This includes 150,000 end-hosts in Campus Manager and 1,200 collectors in IPM.

To manage 5,000 devices for all applications including DFM and HUM, you must set up:

- DFM on a Standalone server (with only CS, Portal, CWA, and DFM installed)
- HUM on a Standalone server (with only CS, Portal, CWA, and HUM installed)
- All other CiscoWorks applications on another server

For HUM, the scaling numbers are:

- All applications installed in a single server with 300 device SKU—15,000 MIB objects.
- All applications installed in a single server with 1500 device SKU—50,000 MIB objects.

Concurrent Users Supported

LMS 3.1 can support:

- 3 concurrent users for LMS 100 and LMS 300 License types.
- 20 concurrent users for LMS 1,500, LMS 5,000 and LMS 10,000 License types.

Multiple number of simultaneous users can affect system performance. 20 concurrent users is the maximum recommended number. However, this depends on the size and configuration of the server.

Licensing Your Product

The LMS 3.1 product provides features such as software-based product registration and license key activation technologies. While installing CiscoWorks, the installer displays the Registration and Licensing input dialog box.

Understanding Product Authorization Key

The Product Authorization Key (PAK) is printed on the software claim certificate. Use the PAK to get your license file from Cisco.com. You may obtain and install your license file at any time while you are working on LMS, not necessarily only at the time you install the product.

We recommend that you complete the LMS license registration and receive the product license before installing LMS 3.1.

License File

When you register your LMS purchase on the product licensing area of Cisco.com, you will receive a license file. You must enter your PAK to receive a license file.

If you are a registered user of Cisco.com, get your license file from: <http://www.cisco.com/go/license>

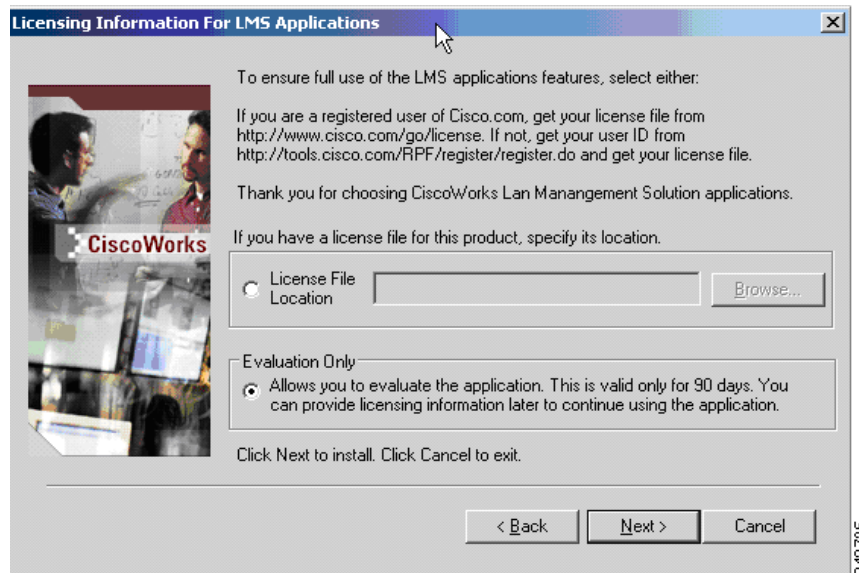
If you are not a registered user of Cisco.com, get your Cisco.com user ID from: <http://tools.cisco.com/RPF/register/register.do>. Once you have obtained your Cisco.com user ID, log on to <http://www.cisco.com/go/license> to get your license file.

Logging in allows your Cisco user profile information to auto-populate many of the product registration fields. Login is case sensitive.

You must enter the license file according to the one you have purchased with the LMS 3.1 product. See [License Information](#) to furnish the appropriate license file.

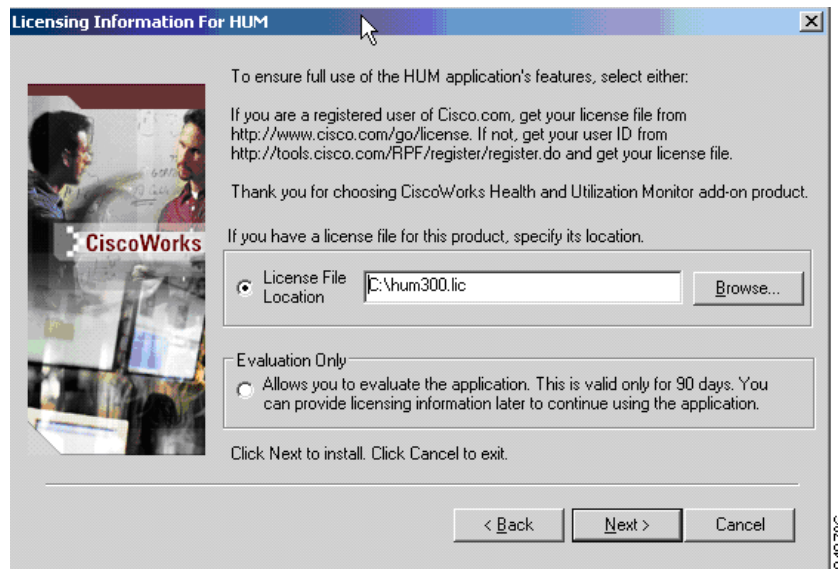
If you have not purchased a license with the product, and if you have only an Evaluation copy, you can select the Evaluation mode and proceed with using the LMS 3.1 product.

[Figure 3-1](#) displays the licensing screen for LMS Applications on Windows operating system.

Figure 3-1 **Licensing Screen for LMS Applications**

The LMS installation program prompts you to enter either the license file or select the Evaluation Only option (see Figure 3-1).

Figure 3-2 displays the licensing screen for HUM on Windows operating system.

Figure 3-2 **Licensing Screen for HUM**

We recommend that you complete the license registration process at this point.

Evaluation Mode

If you have received the LMS as an evaluation copy, you need not register the product during the 90-day evaluation period.

The installation process for an evaluation copy is the same as that of a purchased product, except that you are prompted to select the Evaluation Only option from the Licensing Information page (see [Figure 3-1](#)).

If you choose to run LMS in the evaluation mode, it is valid for only 90 days and does not support any upgrades and allows support for only 100 devices. It stops functioning after 90 days. The evaluation period cannot be extended.

If you have not purchased the product, the LMS evaluation server can be reactivated by purchasing LMS from your authorized Cisco reseller and you can register the product. For details, see [Installing the Licensing File](#).

The behavior of HUM in evaluation mode will be the same as explained above.

NFR (Not For Resale) License

NFR (Not For Resale) License is a default license that is valid for only 365 days. It allows you to manage up to 100 devices.

To install a NFR copy of CiscoWorks applications, you must apply the NFR license either during the installation or after the installation using the graphical user interface.

To apply the NFR license during the installation, you must:

-
- Step 1** Select the License File location option in the Licensing Information page of LMS 3.1 during the installation. See [Figure 3-1](#).
See [Performing Installation of LAN Management Solution 3.1](#) for detailed instructions on installing the product.
 - Step 2** Enter the LMS 3.1 NFR license file location, or click **Browse** to locate the NFR license file.
 - Step 3** Click **OK**.
After specifying the NFR License file for LMS 3.1, the Licensing Information dialog box appears for HUM, if you have selected HUM earlier in the list of applications to be installed. See [Figure 3-2](#).
 - Step 4** Enter the HUM NFR license file location, or click **Browse** to locate the NFR license file.
 - Step 5** Click **OK**.

The System Requirements dialog box appears.

The installation program calculates the minimum disk space, RAM and SWAP space required to install the product.

The required RAM space to install NFR license of the product is 4 GB (4096 MB). The following warning message appears if the RAM space is lesser than 8 GB:

The available RAM is X MB which is lesser than the required RAM of 8192 MB which may affect the performance. Click Yes to proceed or No to abort.

You can ignore this warning message and continue the installation if the RAM space on your server is more than 4 GB.

You can also apply NFR license after the installation is completed.

To apply the NFR license after the installation is completed, you must select the Evaluation Only option in the Licensing Information page while the installation is progressing. See [Figure 3-1](#) and [Figure 3-2](#).

After the installation is completed, you should:

-
- | | |
|---------------|--|
| Step 1 | Launch CiscoWorks. |
| Step 2 | Go to the CiscoWorks home page and select Common Services > Server > Admin > Licensing .
The License Administration page appears. |
| Step 3 | Click Update . |
| Step 4 | Enter the path to the NFR license file in the License field, or click Browse to locate the NFR license file. |
| Step 5 | Click OK to apply the license. |
-

Installing the Licensing File

We recommend that before installing the LMS 3.1 product, you register the product and receive a permanent license.

To license your product, you must:

-
- | | |
|---------------|---|
| Step 1 | Register the LMS product with Cisco.com using the PAK to get your license file. The PAK is printed on the software claim certificate.

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

If you are not a registered user of Cisco.com, get your Cisco.com user ID from: http://tools.cisco.com/RPF/register/register.do . Once you have obtained your Cisco.com user ID, log on to http://www.cisco.com/go/license to get your license file.

Logging in allows your Cisco user profile information to auto-populate many of the product registration fields. Login is case sensitive. After successful registration, you will receive your license file information through an email. |
| Step 2 | After you install LMS 3.1, copy this new license file to the CiscoWorks Common Services server into a directory with read permissions for the user name <i>casuser</i> in the user group <i>casusers</i> . |
| Step 3 | Install the license file.

If you have obtained the LMS license before installation:
<ol style="list-style-type: none">a. Select the first LMS applications you wish to install and when prompted:<ul style="list-style-type: none">– On Windows, select the first radio button (see Figure 3-1) and use the browse window to locate the license file directory.– On Solaris, select L for License File after you accept the Licensing Agreement and continue installing the application.b. Click Next to install the license file. |

After you have completed the LMS install by entering the appropriate license file, if you want to convert an evaluation copy to a licensed copy, perform the following:

- a. Go to the CiscoWorks home page and select **Common Services > Server > Admin > Licensing**.

The License Administration page appears.

- b. Click **Update**.

A file browser popup dialog box appears.

- c. Enter the path to the new license file in the License field, or click **Browse** to locate the license file that you copied to the server in Step 2.

- d. Click **OK**.

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

The updated licensing information appears in the License Information page. If you encounter errors, repeat the steps to license your product.

**Note**

The License file obtained is platform independent and hence can be used in both Windows as well as Solaris operating systems.



CHAPTER 4

Performing Installation of LAN Management Solution 3.1

This chapter describes how to install and uninstall CiscoWorks LMS 3.1 on Solaris and Windows systems.

It describes the tasks you have to perform for upgrade installing CiscoWorks LMS 3.1 on both Solaris and Windows systems. It also helps you to verify the installation, uninstall, and reinstall LMS 3.1.

The installation process is explained in the following sections:

- [Performing New Installation of LMS 3.1](#)
- [Upgrading to LMS 3.1](#)
- [Verifying the Installation](#)
- [Uninstalling LMS 3.1](#)
- [Re-installing LMS 3.1](#)

Performing New Installation of LMS 3.1

LMS3.1 is a minor upgrade version over the LMS3.0 release. The new add-on application, HUM1.1 is bundled along with LMS for the first time.

This section explains how to install LMS 3.1 on Windows and Solaris systems for the first time.

- [Installing LMS 3.1 on Solaris - New](#)
- [Installing LMS 3.1 on Windows - New](#)
- [Installing LMS 3.1 in Silent Mode](#)

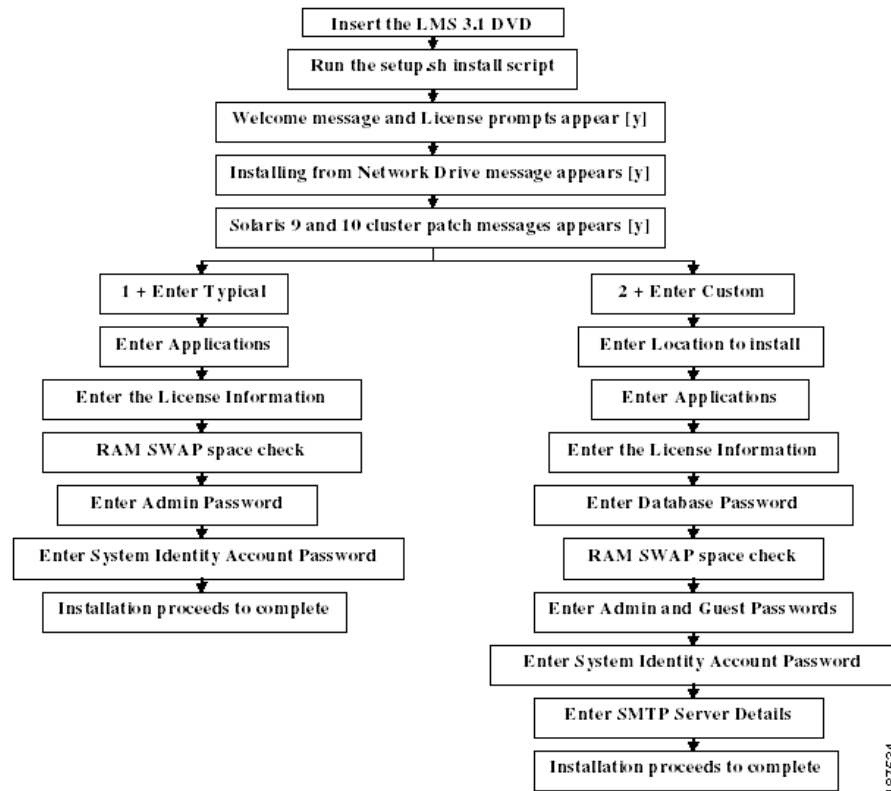
The LMS 3.1 installation program takes approximately an hour and a half to complete on Windows and approximately an hour to complete on Solaris, on a single server with the recommended hardware requirements.

This can take more than two hours if you perform network management integration while installing.

- If Virus Check is enabled in your system, then installation of CiscoWorks applications will take a longer time.
- If HP Openview is running on your system, installation will take a longer time. Disable HP Openview to run a faster installation.

Installing LMS 3.1 on Solaris - New

[Figure 4-1](#) helps you understand the Typical and Custom installation flows in LMS 3.1 on Solaris.

Figure 4-1 LMS 3.1 Installation on Solaris

187534

To install the LMS 3.1 DVD on a Solaris system for the first time:

Step 1 Log into the machine where you want to install LMS 3.1.

Step 2 Insert the LMS 3.1 DVD.

Step 3 Run the installation setup script by entering:

```
# sh setup.sh
```

or

```
# ./setup.sh
```

A Welcome message appears:

```
Welcome to CiscoWorks LAN Management Solution 3.1 Applications setup program.
```

A prompt appears:

```
Press Enter to read/browse the following license agreement:
```

Step 4 Press **Enter** to read the license agreement.

The following message appears at the end of the license agreement:

```
Do you accept all the terms of the License Agreement? (y/n) [n]:
```

Step 5 Enter **Y** to accept the license agreement and proceed with the installation, or enter **N** to deny and quit the installation.



Note

Error messages or warning messages appear if you do not have the required or recommended Server and Client patches.

While installing from the network drive, the Installing from Network Drive message appears.

Installation from the network drive will be slower than installing from the local drive.

If you are installing from a network drive, the installation might take longer to complete. This happens especially for CiscoView device packages.

Step 6 Enter **Y** to proceed or **N** to exit installation.

We recommend you download and install the latest required and recommended patches from <http://www.sun.com>, before you run LMS. For more information on Solaris patches, see [Solaris Patches](#).

The following warning messages appear to ensure you install the Cluster Patches required for Solaris 9:

```
WARNING: Ensure that you have installed the recommended Solaris 9 cluster patches released
on Dec/11/06, in this server.
```

```
WARNING: If these cluster patches are not installed, please download and install them
from http://www.sun.com/.
```

```
WARNING: Otherwise, some features of the CiscoWorks applications will not function
properly.
```

```
Do you want to continue the installation? (y/n) [y]:
```

The following warning messages appear to ensure you install the Cluster Patches required for Solaris 10:

```
WARNING: Ensure that you have installed the recommended Solaris 10 cluster patches
released on Apr/17/07, in this server.
```

```
WARNING: If these cluster patches are not installed, please download and install them
from http://www.sun.com/.
```

```
WARNING: Otherwise, some features of the CiscoWorks applications will not function
properly.
```

```
Do you want to continue the installation? (y/n) [y]:
```

If you enter **Y** and proceed with the installation, a message appears prompting you to select any one mode to install.

Step 7 Select any one of the appropriate installation mode to proceed:

- **Typical** to select the components and install the selected components in the default location (/opt/CSCOpX). This is the default installation mode. See [Installing LMS 3.1 on Solaris —New \(Typical\)](#)
 - **Custom** to select optional components, customize the settings, and to specify the location. See [Installing LMS 3.1 on Solaris — New \(Custom\)](#)
-

Installing LMS 3.1 on Solaris —New (Typical)

To install LMS 3.1 for the first time on a Solaris system using the Typical option:

Step 1 At the command prompt, press either:

- **1** and **Enter** to proceed with the installation after you select the Typical mode.

Or

- **Q** to quit the installation.

If you press **Enter** to proceed with the installation, the installation program performs the prerequisites checks and the following message appears:

Select the applications you want to install.

```
1) Common Services 3.2
2) LMS Portal 1.1
3) CiscoWorks Assistant 1.1
4) CiscoView 6.1.8
5) Integration Utility 1.8
6) Resource Manager Essentials 4.2
7) Campus Manager 5.1
8) Device Fault Manager HPOV-NetView adapters 3.1
9) Device Fault Manager 3.1
10) Internetwork Performance Monitor 4.1
11) All of the above
----Add-on Applications-----
12)Health and Utilization Monitor 1.1
-----
```

Select one or more items using its number separated by comma or enter q to quit:

Make sure you have sufficient disk space. For disk space requirements, see [System and Browser Requirements for Server and Client](#).

Step 2 Enter the number corresponding to the option you have chosen or **q** to quit.

CiscoWorks Common Services 3.2, LMS Portal 1.1 and CiscoWorks Assistant 1.1 are selected by default to be installed. Apart from them, you can select to install other required applications.

You can select more than one component using the corresponding numbers, separated by commas. For example, select 1, 2, 3, 6 to select Common Services, LMS Portal, CiscoWorks Assistant and Resource Manager Essentials.

Integration Utility 1.8 can be installed independently. It does not depend on Common Services 3.2 or LMS Portal 1.1 or any application for installation.

You cannot install or reinstall both DFM 3.1 and DFM 3.1 HPOV- Netview Adapters at the same time. If you select both, DFM 3.1 will be selected by default and a message appears to indicate the same.

After you select the applications, the following message is displayed:

Press **Y** to reselect the components or Enter to proceed? <y/n> [n]:

- Step 3** Press either:
- **Y** to change your selection of applications
 - Or
 - **Enter** to continue with the installation.

The License message appears prompting you to enter the license information for LMS 3.1.

**Note**

If you do not have a license you can select the Evaluation Mode. You must obtain a valid License Key within 90 days.

- Step 4** Enter any of the following:
- **L** and provide the License file location.
 - **E** to opt for an evaluation mode. In this mode, you can provide license information later to fully enable the product.
 - **Q** to quit the installation.

**Note**

You need to specify the License information only when you install either RME, DFM, IPM CM or HUM. You will not encounter this message while installing other applications.

After specifying the License file for LMS 3.1, the License message appears for HUM.

The evaluation copy of HUM is packaged with LMS 3.1 and you need to purchase a separate license to use HUM.

- Step 5** Enter any of the following:
- **L** and provide the License file location.
 - **E** to opt for an evaluation mode. In this mode, you can provide license information later to fully enable the product.
 - **Q** to quit the installation.

If you specify the license file for HUM, the following message appears:

```
You have opted to install the licensed version of CiscoWorks HUM 1.1. To use this application, ensure that you have a licensed version of LMS 3.1.
```

The above message implies that you can install the licensed version of HUM only over a licensed version of LMS.

If you choose the evaluation option, the following message appears:

```
You have opted to evaluate CiscoWorks HUM 1.1. This is valid only for 90 days. If you provide the licensing information later, ensure that you have installed a licensed version of LMS 3.1, to continue using the application.
```

The installation program calculates the minimum disk space, RAM and SWAP space required for installing the product.

If the disk space is sufficient, the following message appears:

```
Sufficient disk space.
```

If the drive does not have enough space, an error message appears and the installation exits.

- Step 6** Enter the CiscoWorks Admin password and confirm it.
- For more information on passwords, see [Password Information](#).

Step 7 Enter the System Identity Account Password and confirm it.

This password will be used on all multi-server machines.

A message appears:

```
Do you want to see the passwords that were entered/randomly generated? (y/n) [n]
```

The Device Fault Manager uses a data transport protocol that requires authentication for server-to-server communication. You can retain the existing username and password for securing this interface.

Step 8 Enter **y**.

The following message appears:

```
WARNING: Exiting installation beyond this point might result in system instability.
```

```
Do you want to continue the installation? (y/n) [y]:
```

Step 9 Enter **y**.

Installation now proceeds. It takes approximately an hour to complete the installation.

At the end of installation, the following messages appear if the respective applications were installed:

```
WARNING: To ensure that you have the latest device support for RME,
```

```
WARNING: please install the latest Device Packages from Cisco.com @
```

```
WARNING: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme
```

```
WARNING: Please refer to the Installing and Getting Started with CiscoWorks LAN Management  
Solution 3.1 guide for details.
```

The above message appears only if you have installed RME.

```
WARNING: To ensure that you have the latest device support for CM,
```

```
WARNING: please install the latest Device Packages from Cisco.com @
```

```
WARNING: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-campus
```

```
WARNING: Please refer to the Installing and Getting Started with CiscoWorks LAN Management  
Solution 3.1 guide for details.
```

The above message appears only if you have installed CM.

```
WARNING: To ensure that you have up-to-date device support,
```

```
WARNING: install the latest Service Pack (SP) from Cisco.com, at
```

```
WARNING: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm.
```

```
WARNING: For installation details, refer to the Installing and Getting Started with  
CiscoWorks LAN Management Solution 3.1 guide.
```

The above message appears only if you have installed DFM.

The installation completes without displaying more questions and the system prompt appears.

The following messages appear at the end of the installation:

```
Software Installation Tool Completed
```

```
Possible Warnings/Errors Encountered
```

The warning and error messages that appear after these messages do not hinder the installation. They only indicate that you need to take corrective actions after the installation has completed.

Your Solaris machine has the selected applications of LMS 3.1 installed successfully.

**Note**

On Solaris 10 if you have selected to install DFM, a warning message may appear prompting you to reboot the machine at the end of installation. If the settings required by DFM are already available, the message may not appear.

**Note**

If cluster patches are installed for Solaris 10, you must reboot your system after installing LMS.

To prepare the client system for use, see [System and Browser Requirements for Server and Client](#).

For troubleshooting information, see [Checking Processes After Installation](#) and [Understanding Installation Error Messages](#).

Installing LMS 3.1 on Solaris — New (Custom)

To install LMS 3.1 for the first time on a Solaris system using the Custom option:

Step 1 Go to the command prompt and select either:

- **2** and **Enter** to proceed with the installation after you select the Custom mode.

Or

- **Q** to quit the installation.

If you select **Enter** to proceed with the installation, the following message appears:

Enter the location where the product will be installed. The default location is /opt/CSCOpX. If you choose another location, installation will create a symbolic link /opt/CSCOpX to that location.

Destination folder should not contain the following characters:

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

Enter location or q to quit [/opt/CSCOpX]:

The Custom path or location you specify cannot be the sub-directory of /opt/CSCOpX.

**Caution**

Do not remove the link after installation. LMS will not work without this symbolic link.

Step 2 Press **Enter** to accept the default directory for product installation, or enter another directory.

Select the applications you want to install.

- 1) Common Services 3.2
- 2) LMS Portal 1.1
- 3) CiscoWorks Assistant 1.1
- 4) CiscoView 6.1.8
- 5) Integration Utility 1.8
- 6) Resource Manager Essentials 4.2
- 7) Campus Manager 5.1
- 8) Device Fault Manager HPOV-NetView adapters 3.1
- 9) Device Fault Manager 3.1

```

10) Internetwork Performance Monitor 4.1
11) All of the above
-----Add-on Applications-----
12) Health and Utilization Monitor 1.1
-----

```

Select one or more items using its number separated by comma or enter **q** to quit:

Make sure you have sufficient disk space. For disk space requirements, see [System and Browser Requirements for Server and Client](#).

Step 3 Enter the number corresponding to the option you have chosen or **q** to quit.

CiscoWorks Common Services 3.2, LMS Portal 1.1 and CiscoWorks Assistant 1.1 are selected by default to be installed. Apart from them, you can select to install other required applications.

You can select more than one component using the corresponding numbers, separated by commas. For example, select 1, 2, 3, 6 to select Common Services, LMS Portal, CiscoWorks Assistant and Resource Manager Essentials.

Integration Utility 1.8 can be installed independently. It does not depend on Common Services 3.2 or LMS Portal 1.1 or any application for installation.

You cannot install or reinstall both DFM 3.1 and DFM 3.1 HPOV- Netview Adapters at the same time. If you select both, DFM 3.1 will be selected by default and a message appears to indicate the same.

Press **Y** to reselect the components or Enter to proceed? <y/n> [n]:

Step 4 Press either:

- **Y** to change your selection of applications
- Or
- **Enter** to continue with the installation.

The License message appears prompting you to enter the license information.



Note

If you do not have a license you can select the Evaluation Mode. You must obtain a valid License Key within 90 days.

Step 5 Enter any of the following:

- **L** and provide the License file location
- **E** for an evaluation mode. In this mode, you can provide license information later to fully enable the product.
- **Q** to quit the installation.

You need to specify the License information only if you are installing either RME, DFM, IPM CM or HUM. You will not encounter this message while installing other applications.

After specifying the License file for LMS 3.1, the Database Password prompt appears.

Step 6 Enter the database password.

This password will be used internally by the product. It must begin with an alphabet and have less than 15 characters.

For more information on passwords, see [Password Information](#).

The license prompt for HUM appears.

The evaluation copy of HUM is packaged with LMS 3.1 and you need to purchase a separate license to use HUM.

Step 7 Enter any of the following:

- **L** and provide the License file location.
- **E** to opt for an evaluation mode. In this mode, you can provide license information later to fully enable the product.
- **Q** to quit the installation.

If you specify the license file for HUM, the following message appears:

```
You have opted to install the licensed version of CiscoWorks HUM 1.1. To use this application, ensure that you have a licensed version of LMS 3.1.
```

The above message implies that you can install the licensed version of HUM only over the licensed version of LMS.

If you choose the evaluation option, the following message appears:

```
You have opted to evaluate CiscoWorks HUM 1.1. This is valid only for 90 days. If you provide the licensing information later, ensure that you have installed a licensed version of LMS 3.1, to continue using the application.
```

The installation program calculates the minimum disk space, RAM and SWAP space required for installing the product.

- If the disk space is sufficient, the following message appears:
Sufficient disk space.
- If the drive does not have enough space, an error message appears and the installation exits.

Step 8 Enter the CiscoWorks Admin password and confirm it.

For more information on passwords, see [Password Information](#).

Step 9 Enter the Guest password and confirm it.

For more information on passwords, see [Password Information](#).

Step 10 Enter the System Identity Account password and confirm it.

In a multi-server environment, you must configure all systems part of your multi-server setup with the same System Identity Account password.

For more information on passwords, see [Password Information](#).

Step 11 Enter the SMTP server name. For more information, see [License Information](#).

Step 12 Enter the country code, state, city, company, organization, administrator's e-mail address, and host name for HTTPS.

Only the Host name is mandatory. Other fields are optional. Press **Enter** to skip other fields.

Step 13 Enter either:

- **N** not to integrate with a third-party NMS after installation. This completes the installation faster. It also avoids errors that may be caused by third-party integration.

Or

- **Y** to integrate with a third-party NMS during installation.

If you select **Y**:

a. Select any of the following:

- The adapter from the list of available adapters.
- **Other** to choose an adapter that is not listed (you are prompted to enter the path name of the adapter).
- **None** to integrate after the installation is complete.

If you select **None**, go to [Step 14](#).

Many third-party products allow you to launch CiscoWorks applications from within the third-party product. The CiscoWorks applications are launched in a web browser.

b. Enter the full pathname for the web browser.

A message appears prompting you to enable download updates to NMIDB (Network Management Integration Data Bundle) directly from Cisco.com.

c. Select either:

- **N** to disable future updates from Cisco.com.
- **Y** to enable future updates from Cisco.com.

If you select **N**, go to [Step 14](#).

d. Enter your Cisco.com user ID and password.

You must have Cisco.com login privileges. If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the standard Cisco.com web site.

The installation program checks dependencies and system requirements and copies the files to the run time (local directory) and the installation proceeds.

A message appears:

Do you want to see the passwords that were entered/randomly generated? (y/n) [n]

The Device Fault Manager uses a data transport protocol that requires authentication for server-to-server communication. You can retain the existing username and password for securing this interface.

Step 14 Enter **Y**.

A message appears:

Exiting installation beyond this point might result in system instability.

Do you want to continue the installation? (y/n) [y]

Step 15 Enter Y.

Installation now proceeds. At the end of installation, the following messages appear:

```
WARNING: To ensure that you retain the latest device support for RME,  
WARNING: please install the latest Device Packages from Cisco.com @  
WARNING: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme  
WARNING: Please refer to the Installing and Getting Started with CiscoWorks LAN Management  
Solution 3.1 guide for details.
```

The above message appears only if you have installed RME.

```
WARNING: To ensure that you retain the latest device support for CM,  
WARNING: please install the latest Device Packages from Cisco.com @  
WARNING: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-campus  
WARNING: Please refer to the Installing and Getting Started with CiscoWorks LAN Management  
Solution 3.1 guide for details.
```

The above message appears only if you have installed CM.

```
WARNING: To ensure that you have up-to-date device support,  
WARNING: install the latest Service Pack (SP) from Cisco.com, at  
WARNING: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm.  
WARNING: For installation details, refer to the Installing and Getting Started with  
CiscoWorks LAN Management Solution 3.1 guide.
```

The above message appears only if you have installed DFM.

The installation completes without displaying more questions and the system prompt appears.

It takes approximately an hour to complete the installation.

The following messages appear at the end of the installation:

```
Software Installation Tool Completed  
Possible Warnings/Errors Encountered
```

The warning and error messages that appear after these messages do not hinder the installation. They only indicate that you need to take corrective actions after the installation has completed.

Your Solaris machine has the selected applications of LMS 3.1 installed successfully.

**Note**

On Solaris 10 if you have selected to install DFM, a warning message may appear prompting you to reboot the machine at the end of installation. If the settings required by DFM are already available, the message may not appear.

**Note**

If cluster patches are installed for Solaris 10, you must reboot your system after installing LMS.

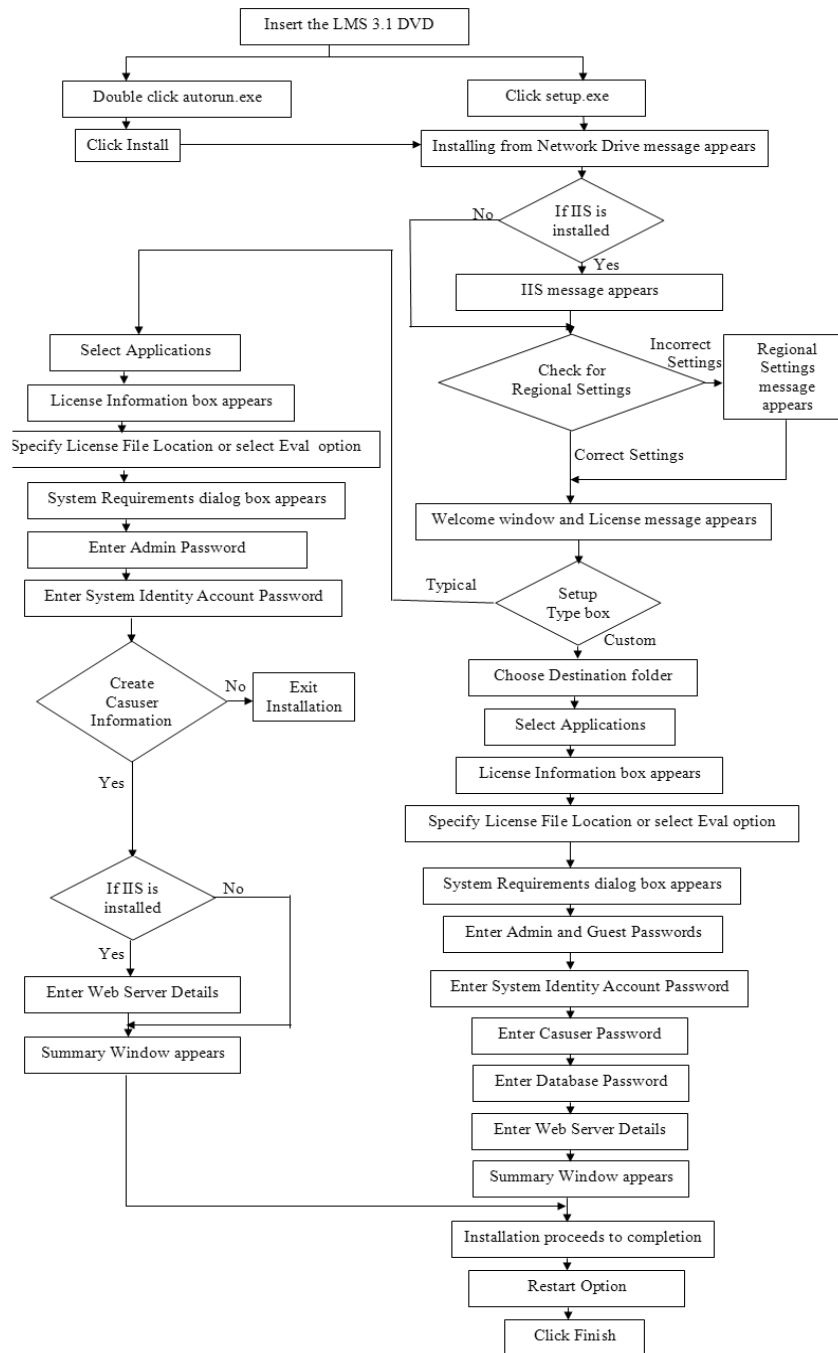
To prepare the client system for use, see [System and Browser Requirements for Server and Client](#).

For troubleshooting information, see [Checking Processes After Installation](#) and [Understanding Installation Error Messages](#).

Installing LMS 3.1 on Windows - New

Figure 4-2 helps you understand the Typical and Custom installation flows in LMS 3.1 on Windows.

Figure 4-2 LMS 3.1 Installation On Window



187777

To install LMS 3.1 on a Windows system for the first time:

Step 1 Login as administrator to the machine where you want to install LMS 3.1.

- a. Insert the LMS 3.1 DVD.
- b. Double-click on the autorun.exe or setup.exe file.

The CiscoWorks LAN Management Solution 3.1 Applications window appears.

- c. Click **Install** to continue.

While installing from the network drive, the Installing from Network Drive window appears.

Installation from network drive will be slower than installing from the local drive.

Step 2 Click **Yes** to proceed or **No** to exit installation.

The Internet Information Services (IIS) detection message appears.

When Internet Information Services (IIS) is detected on your system and if you have continued the installation without IIS services, you cannot use the port number 443 for HTTPS.

Instead, you must use the port numbers ranging from 1026 to 65535 for HTTPS to avoid this conflict.

Step 3 Click **Yes** or **No** to continue.

Installation checks for the Regional Settings. They have to be set either as US English or Japanese.

If the Primary settings point to an unsupported locale, the following warning message appears:

You are trying to install CiscoWorks on an unsupported locale. CiscoWorks supports only US English or Japanese languages. Please reinstall your Operating System with a supported locale and change the Regional Settings to either of these languages.

Click Yes to continue installing CiscoWorks or No to exit.

Step 4 Click:

- **Yes** to continue the installation
- **No** to terminate the installation.

You can install LMS after re-installing the Operating System with the supported locale.

If the Active settings point to an unsupported locale, the following warning message appears:

You are trying to install CiscoWorks on an unsupported locale. CiscoWorks supports only US English or Japanese languages. Please change the Regional Settings to either of these languages.

Click Yes to continue installing CiscoWorks or No to exit.

Step 5 Click:

- **Yes** to continue the installation
- **No** to terminate the installation.

You can install LMS after correcting the Active regional settings in **Control Panel > Regional and Language Options > Regional Options**.

The Welcome window appears.

Step 6 Click **Next** to continue.

The Software License Agreement window appears. You must accept this agreement to install CiscoWorks LMS 3.1.

Step 7 Click **Accept** to continue.

If you are trying to install on an unsupported platform, the following error message appears:

You cannot install CiscoWorks LMS 3.1 application(s) on an unsupported operating system or when Terminal Services is running on the supported Windows 2003 Server Standard Edition, Windows 2003 Server Enterprise Edition, and Windows 2003 R2 Server platforms

The setup program will exit when you click OK

You must either upgrade the operating system on the server to a supported version or install LMS 3.1 application(s) on another server that runs a supported operating system.

You cannot install LMS 3.1 on Windows 2000 server platform. You need to upgrade to Windows 2003 operating system and then continue with installation. If not, installation will terminate.

When you have the recommended platform, the installation continues.

If you are trying to install CiscoWorks Common Services on a Primary Domain Controller or Backup Domain Controller, installation terminates after showing the following error message:

You are attempting to install CiscoWorks Common Services 3.2 on a server that is configured as a Primary Domain Controller or a Backup Domain Controller (PDC/BDC).

Install CiscoWorks Common Services 3.2 on another server not configured as PDC / BDC.

The Setup Type dialog box appears.

Step 8 Select one of the following:

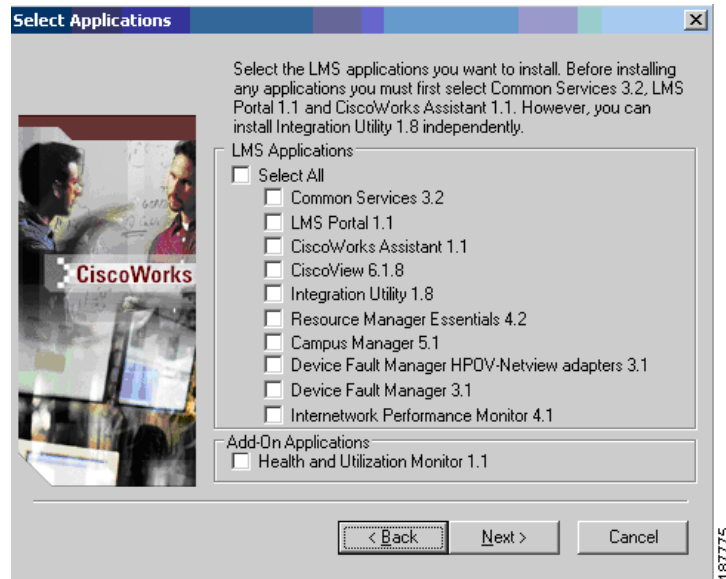
- **Typical** to select the components and install the selected components in the default location (*System Drive\Program Files\CSCOPx*). This is the default installation mode. See [Installing LMS 3.1 on Windows — New \(Typical\)](#)
 - **Custom** to select the components, customize the settings, and to specify the location. See [Installing LMS 3.1 on Windows —New \(Custom\)](#)
-

Installing LMS 3.1 on Windows — New (Typical)

To install LMS 3.1 for the first time on a Windows system using the Typical option:

- Step 1** Click **Next** to continue after you select the Typical installation mode.
The Select Applications dialog box appears as given in [Figure 4-3](#):

Figure 4-3 Select Applications Dialog box in New Installation



CiscoWorks Common Services 3.2, LMS Portal 1.1 and CiscoWorks Assistant 1.1 are selected by default to be installed. You can select to install the other required applications.

You can select the required applications by checking the corresponding check-boxes.

Integration Utility 1.8 can be installed independently. It does not depend on Common Services 3.2 or LMS Portal 1.1 or any application for installation.

You cannot install or reinstall both DFM 3.1 and DFM 3.1 HPOV- Netview Adapters at the same time. If you select both, DFM 3.1 will be selected by default and a message appears to indicate the same.

- Step 2** Click **Next** after selecting the applications to install and continue.

The Licensing Information dialog box appears for LMS 3.1.

- Step 3** Specify the License File Location.

If you do not have a license you can select the Evaluation Mode. You must obtain a valid License Key within 90 days.



Note

You need to specify the License information only when you install either RME, DFM, IPM, CM or HUM. You will not encounter this message while installing other applications.

After specifying the License file for LMS 3.1, the Licensing Information dialog box appears for HUM.

The evaluation copy of HUM is packaged with LMS 3.1 and you need to purchase a separate license to use HUM.

Step 4 Specify the License File Location or select the Evaluation option.

- If you specify the license file for HUM, the following message appears:

You have opted to install the licensed version of CiscoWorks HUM 1.1. To use this application, ensure that you have a licensed version of LMS 3.1.

The above message implies that you can install the licensed version of HUM over the licensed version of LMS.

- If you choose the evaluation option, the following message appears:

You have opted to evaluate CiscoWorks HUM 1.1. This is valid only for 90 days. If you provide the licensing information later, ensure that you have installed a licensed version of LMS 3.1, to continue using the application.

Step 5 Click **OK**.

The System Requirements dialog box appears.

The Installation program checks the system configuration and required space.

Step 6 Click **Next**.

The Change Admin Password box appears.

Step 7 Enter the User Admin password and confirm it.

For more information on passwords, see [Password Information, page A-7](#).

Step 8 Click **Next** to continue installation.

The Change System Identity Account password dialog box appears.

Step 9 Enter the System Identity Account password and confirm it.

In a multi-server environment, you must configure all systems that are part of your multi-server setup with the same System Identity Account password.

For more information on passwords, see [Password Information, page A-7](#).

Step 10 Click **Next**.

The Create casuser information box appears.

Casuser is the user who administers and maintains CiscoWorks Server, without having administrative privileges.

Step 11 Click **Yes** to continue with installation or **No** to abort.

The Web Server dialog box appears.

Step 12 Enter HTTPS port, server administrator e-mail address, and the SMTP server name.

The HTTPS port and SMTP server name are mandatory.

The default HTTPS port number is 443. The SMTP server name is used by other CiscoWorks applications.



Note

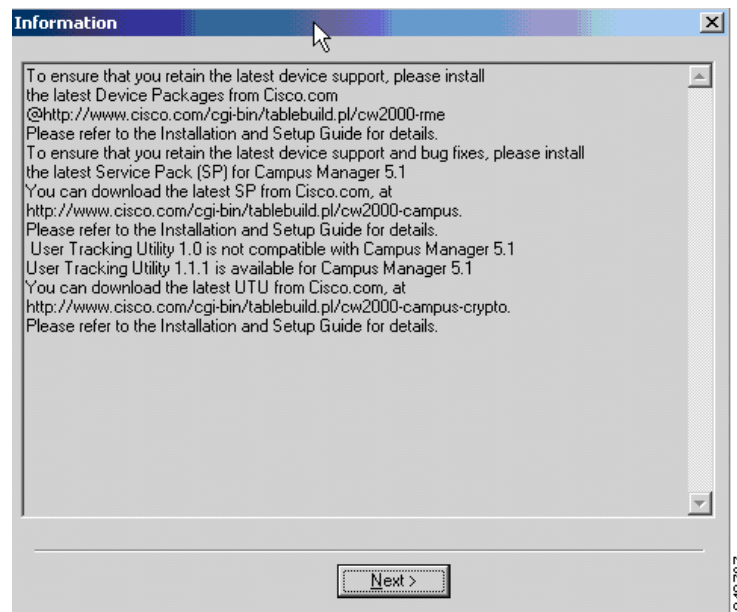
When IIS is detected on your system, to avoid any conflict with HTTPS, you need to use different port numbers for HTTPS ranging from 1026 to 65535.

Step 13 Click **Next**.

Installation continues.

At the end of installation, based on the applications you have selected to install or reinstall, warning messages appear. These messages prompt you to install the latest device updates as indicated in [Figure 4-4](#).

Figure 4-4 Device Updates Information

**Step 14** Click **OK** and proceed to complete the installation.

Information about the various LMS applications, their features and benefits are displayed during installation.

The Restart dialog box appears after the installation is complete.

You need to restart your machine after you have installed LMS 3.1.

Step 15 Select **Yes, I want to restart my computer now**.**Step 16** Click **Finish**.

To prepare the client system for use, see [System and Browser Requirements for Server and Client](#), page 2-2.

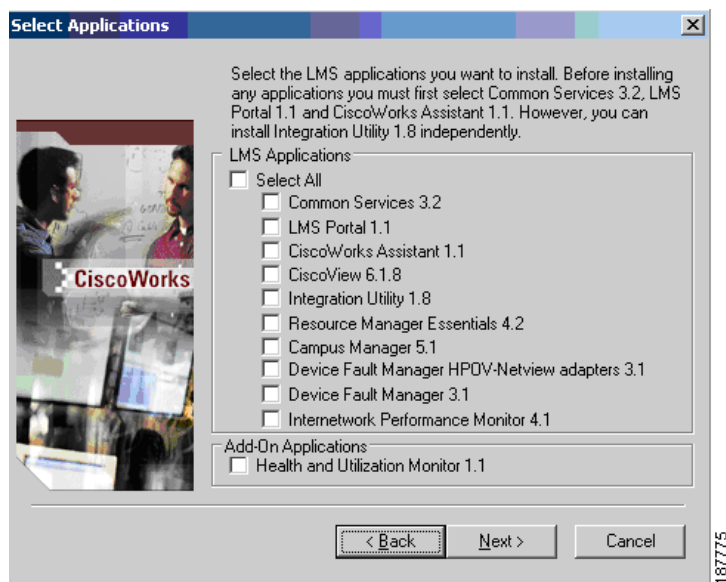
For troubleshooting information, see [Checking Processes After Installation](#), page 6-1 and [Understanding Installation Error Messages](#), page 6-5.

Installing LMS 3.1 on Windows —New (Custom)

To install LMS 3.1 for the first time on a Windows system using the Custom option:

- Step 1** Click **Next** to continue after you select the Custom installation mode.
The Choose Destination Folder dialog box appears.
The default folder is SystemDrive:\Program Files\CSCOpX. You can choose the destination folder where CiscoWorks will be installed.
- Step 2** Click **Next**.
The Change Destination Folder dialog box appears if the destination folder location was entered in Step 1.
You can either select a new destination folder or confirm the one that you selected earlier.
- Step 3** Click **Next** to proceed.
The Select Applications dialog box appears as given in [Figure 4-5](#):

Figure 4-5 *Select Applications Dialog box in New Installation*



CiscoWorks Common Services 3.2, LMS Portal 1.1 and CiscoWorks Assistant 1.1 are selected by default to be installed. Apart from them, you can select to install other required applications.

You can select the required applications by checking the corresponding check-boxes.

Integration Utility 1.8 can be installed independently. It does not depend on Common Services 3.2 or LMS Portal 1.1 or any application for installation.

You cannot install or reinstall both DFM 3.1 and DFM 3.1 HPOV- Netview Adapters at the same time. If you select both, DFM 3.1 will be selected by default and a message appears to indicate the same.

- Step 4** Click **Next** after selecting the applications to install and continue.
The Licensing Information dialog box appears for LMS 3.1.

Step 5 Specify the License File Location.

If you do not have a license you have the option of selecting the Evaluation Mode. You must obtain a valid License file within 90 days.

**Note**

You need to specify the License information only if you are installing either RME, DFM, IPM or CM. You will not encounter this message while installing other applications.

After specifying the License file for LMS 3.1, the Licensing Information dialog box appears for HUM. The evaluation copy of HUM is packaged with LMS 3.1 and you need to purchase a separate license to use HUM.

Step 6 Specify the License File Location or select the Evaluation option.

- If you specify the license file for HUM, the following message appears:

You have opted to install the licensed version of CiscoWorks HUM 1.1. To use this application, ensure that you have a licensed version of LMS 3.1.

The above message implies that you can install the licensed version of HUM only over the licensed version of LMS.

- If you choose the evaluation option, the following message appears:

You have opted to evaluate CiscoWorks HUM 1.1. This is valid only for 90 days. If you provide the licensing information later, ensure that you have installed a licensed version of LMS 3.1, to continue using the application.

Step 7 Click **OK**.

The System Requirements dialog box appears.

The installation program checks the system configuration and required space.

Step 8 Click **Next**.

The Change Admin and Guest Password box appears.

Step 9 Enter user admin and user guest passwords and confirm them.

For more information on passwords, see [Password Information, page A-7](#).

Step 10 Click **Next** to continue installation.

The Change System Identity Account password dialog box appears.

Step 11 Enter the System Identity Account password and confirm it.

In a multi-server environment, you must configure all systems that are a part of your multi-server setup with the same System Identity Account password.

For more information on passwords, see [Password Information, page A-7](#).

Step 12 Click **Next**.

The Change casuser Password dialog box appears.


Casuser is the user who can administer and maintain CiscoWorks Server even without administrative privileges.

Step 13 Enter the casuser password and confirm it.

If you do not enter a password, the installation program generates a random password and adds the new user casuser and the new group casusers to the system.

Step 14 Click **Next** to continue.

The Database Password dialog box appears.

- Step 15** Enter the database password.
- This password will be used internally by the product. It must begin with an alphabet and have less than 15 characters.
- For more information on passwords, see [Password Information, page A-7](#).
- Step 16** Click **Next**.
- The Web Server dialog box appears.
- Step 17** Enter HTTPS port, server administrator e-mail address, and the SMTP server name.
- The default HTTPS port number is 443. The SMTP server name is used by other CiscoWorks applications. The HTTPS port and SMTP server name are mandatory.
-  **Note** When IIS is detected on your system, to avoid any conflict with HTTPS, you need to use different port numbers for HTTPS ranging from 1026 to 65535.
-
- Step 18** Click **Next** to continue installation.
- The Self-Signed Certificate dialog box appears. The webserver uses the self-signed certificate while operating in secure mode.
- Step 19** Enter the country code, state, city, company, organization, and host name for HTTPS.
- The host name is mandatory.
- Step 20** Click **Next** to continue installation.
- The Summary window appears with the updates that will be installed and the settings for the installation.
- Step 21** Click **Next** to continue installation.
- At the end of installation, based on the applications you have selected to install or reinstall, warning messages appear. These messages prompt you to install the latest device latest updates as indicated in [Figure 4-4](#).
- Step 22** Click **OK** and proceed to complete the installation.
- Information about the various LMS applications, their features and benefits are displayed during installation.
- The Restart dialog box appears after the installation is complete.
- You must restart your machine after you have installed LMS 3.1.
- Step 23** Select **Yes, I want to restart my computer now**.
- Step 24** Click **Finish**.
-

To prepare the client system for use, see [System and Browser Requirements for Server and Client](#).

For troubleshooting information, see [Checking Processes After Installation](#) and [Understanding Installation Error Messages](#).

Installing LMS 3.1 in Silent Mode

Silent installation or unattended installation is supported in the LMS single installer. You can perform only a fresh installation of LMS 3.1 in silent installation mode.

Silent install does not prompt for your inputs. It continues the installation based on your inputs provided in a file. You should save the installation inputs in a file and store the file in the system. See [Creating an Answer File](#) for more information.

To install LMS 3.1 in silent mode:

-
- Step 1** Insert the LMS 3.1 DVD.
- Step 2** Navigate to images/disk1 directory at the command prompt.
- Step 3** Enter the following commands to install LMS 3.1 in silent mode:
- On Solaris: `sh setup.sh -q answer_file_name`
 - On Windows: `setup.exe QUIET answerfile=answer_file_name`

where *answer_file_name* is the full path of the user input file stored on the system.

The installation starts.

- Step 4** Restart your system after the installation is complete.
-

Creating an Answer File

The answer file is an ASCII file that provides the required inputs for quiet installations.

The answer file contains the following name=value pairs:

Property	Description
destination	Optional. Allows quiet installation to install into a directory other than <i>NMSROOT</i> . If not specified, installation goes into /opt/CSCOpX on Solaris or c:\Program Files\CSCOpX on Windows.
adminPassword	Specifies the login password for the admin user. This is mandatory.
secretPassword (Solaris only)	Specifies the login password for the secret user.

casuser (Windows Only)	<p>If casuser password does not exist by the time of installation, the framework generates random password for casuser.</p> <ul style="list-style-type: none"> • If the random password is successful, then no input is required. • If the random password fails, installation opens a dialog requesting new password. <p>In quiet mode, installation attempts to load the casuser password from the answer file. If no casuser password is specified in the answer file, installation attempts random password, and might fail if the random password does not pass the company policy.</p>
systemIdentityAccountPassword (Windows only)	Password for the System Identity Account. This is mandatory.

Sample Answer Files

On Windows:

```
#--- begin answer file
#--- hash sign (#) is allowed to mark comments
systemIdentityAccountPassword=admin
casuser=casuser
destination=C:\PROGRA~1\CSCOpX
adminPassword=admin
#--- end of answer file
```

On Solaris:

```
#cat /tmp/answer_file
##Sample Answer file
adminPassword=admin
secretPassword=admin
destination=/opt/CSCOpX
```


Upgrading to LMS 3.1

The following upgrade paths are supported:

LMS Version	Upgrade Path
<ul style="list-style-type: none"> LMS 1.x LMS 2.0 LMS 2.1 	Upgrade to LMS 3.1 is not supported. You should perform a fresh installation of LMS 3.1.
<ul style="list-style-type: none"> LMS 2.2 	<p>You cannot directly upgrade to LMS 3.1. The suggested upgrade path is:</p> <ul style="list-style-type: none"> Remote Upgrade to LMS 2.6/LMS 3.0 <p>OR</p> <p>Local Upgrade to LMS 2.6</p> <ul style="list-style-type: none"> Upgrade to LMS 3.1
<ul style="list-style-type: none"> LMS 2.5 LMS 2.5.1 	<p>You cannot directly upgrade to LMS 3.1. The suggested upgrade path is:</p> <p>LMS 2.5/LMS 2.5.1 > LMS 2.6 > LMS 3.1</p>
<ul style="list-style-type: none"> LMS 2.6 LMS 2.6 SP1 LMS 3.0 LMS 3.0 December 2007 Update 	<p>You can perform a local or remote upgrade to LMS 3.1.</p> <p>For remote upgrade, you should have the same Operating System on both machines.</p>

This section contains information on:

- [Local Upgrade to LMS 3.1 on Solaris](#)
- [Remote Upgrade to LMS 3.1 on Solaris](#)
- [Local Upgrade to LMS 3.1 on Windows](#)
- [Remote Upgrade to LMS 3.1 on Windows](#)

Local Upgrade to LMS 3.1 on Solaris

To upgrade to LMS 3.1 on the same Solaris machine, you can select the relevant option from the following:

- Customers having LMS 2.5 or LMS 2.5.1, must first install LMS 2.6, available from Cisco.com and then proceed to upgrade LMS 3.1 from the DVD.

The LMS 2.6 is available at the location:

<http://www.cisco.com/cgi-bin/tablebuild.pl/lms26>.

For install instructions, see the Readmes at:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html.

- Customers upgrading from LMS 2.6, LMS 2.6 SP1, LMS 3.0 and LMS 3.0 December 2007 update can directly upgrade to LMS 3.1.

**Note**

We recommend that you take a backup of your data before you start the upgrade.

To upgrade to LMS 3.1 on the same Solaris machine:

Step 1 Login as root to the machine where LMS 2.6, LMS 2.6 SP1, LMS 3.0 or LMS 3.0 December 2007 update is already installed.

Step 2 Insert the LMS 3.1 DVD.

Step 3 Run the installation setup script by entering:

```
# sh setup.sh
```

or

```
# ./setup.sh
```

When you upgrade from a LMS 3.0 machine, that has the evaluation version of HUM installed, the following message appears:

You have opted to upgrade the LMS version from 3.0 to 3.1. If you have an evaluation version of HUM, ensure that you uninstall the evaluation version before upgrading. If you have a valid license for HUM, ensure that you apply the license before upgrading.

Do the following:

- Uninstall the evaluation version of HUM. For details, see [Uninstalling LMS 3.1 on Solaris](#)
- Repeat Step 3.

OR

Apply the license for HUM and proceed with the upgrade.

A Welcome message appears:

```
Welcome to CiscoWorks LAN Management Solution 3.1 Applications setup program.
```

A prompt appears:

```
Press Enter to read/browse the following license agreement:
```

Step 4 Press **Enter** to read the License Agreement.

The following message appears at the end of the license agreement:

```
Do you accept all the terms of the License Agreement? (y/n) [n]:
```

Step 5 Enter **Y** to accept the License Agreement and proceed with the installation.

Or

Enter **N** to deny and quit the installation.

The following message appears at the end of the License Agreement:

You must accept this License Agreement to proceed with the installation.

If you enter N/n, the installation will exit.

Do you accept all the terms of the License Agreement? (y/n) [n]:

Do you want to proceed? (y/n) [y]:

If you are installing the image from a network drive, a message appears indicating that installation will be slower when compared to installing from the local drive. This happens especially for CiscoView device packages.

Step 6 Enter **y** to continue.

The following backup prompt appears:

Enter the backup directory:

Step 7 Specify the directory where the backup is to be stored.

Error messages or warning messages appear if you do not have the required or recommended Server and Client patches.

We recommend you download and install the latest required and recommended patches from <http://www.sun.com> before you run LMS applications. For more information on Solaris patches, see [Solaris Patches](#).

If any of the required Server patches is missing, warning messages appear.

The following warning messages appear to ensure you install the Cluster Patches required for Solaris 9:

WARNING: Ensure that you have installed the recommended Solaris 9 cluster patches released on Dec/11/06, in this server.

WARNING: If these cluster patches are not installed, please download and install them from <http://www.sun.com/>.

WARNING: Otherwise, some features of the CiscoWorks applications will not function properly.

Do you want to continue the installation? (y/n) [y]:

The following warning messages appear to ensure you install the Cluster Patches required for Solaris 10:

WARNING: Ensure that you have installed the recommended Solaris 10 cluster patches released on Apr/17/07, in this server.

WARNING: If these cluster patches are not installed, please download and install them from <http://www.sun.com/>.

WARNING: Otherwise, some features of the CiscoWorks applications will not function properly.

Do you want to continue the installation? (y/n) [y]:

If you enter **Y** and proceed with the installation, the following message appears prompting you to select the type of setup for installation.

Choose the type of Setup you prefer.

1) Typical installation. For most users.

Select components to be installed.

Enter Admin and System Identity Account passwords for new installation.

Generates Guest, Database passwords. Retains them for upgrade and reinstallation.

2) Custom installation. For advanced users.

Select components to be installed.

Enter Admin, Guest, System Identity Account, Database passwords for new installation.

Retains them for upgrade and reinstallation.

Select one of the installation modes using its number or (q) to quit [1]:

Step 8 Select the appropriate mode of upgrade installation.

You can perform an upgrade install LMS 3.1 using either the Typical or Custom mode:

- **Typical** to choose the components and install the selected components in the default location (/opt/CSCOpX). This is the default installation mode. See the section, [Local Upgrade to LMS 3.1 on Solaris — Typical](#)
- **Custom** to choose the components, customize the settings, and to specify the location. See the section, [Local Upgrade to LMS 3.1 on Solaris — Custom](#)

Local Upgrade to LMS 3.1 on Solaris — Typical

To perform a local upgrade to LMS 3.1 on a Solaris machine, using the Typical option:

Step 1 Go to the command prompt and select either:

- **1** and **Enter** to proceed with the installation after you select the Typical mode.

Or

- **Q** to quit the installation.

If you press **Enter** a list of the applications appears.

1) Common Services 3.2

2) LMS Portal 1.1

3) CiscoWorks Assistant 1.1

4) CiscoView 6.1.8

5) Integration Utility 1.8

6) Resource Manager Essentials 4.2

7) Campus Manager 5.1

8) Device Fault Manager HPOV-NetView adapters 3.1

9) Device Fault Manager 3.1

10) Internetwork Performance Monitor 4.1

11) All of the above

-----Add-on Applications-----

12) Health and Utilization Monitor 1.1

You can select and install one or more applications. By default the applications you installed in the earlier version of LMS appear as selected for upgrade.

Step 2 Enter the number corresponding to the option you have chosen or **Q** to quit.

Make sure you have sufficient disk space. For disk space requirements, see [System and Browser Requirements for Server and Client](#).

The existing applications in the earlier version of LMS, are upgraded to their latest versions by default when you install LMS 3.1.

You can select more than one application. To do this enter the numbers of the options, separated by commas.

After you select the applications, the following message is displayed:

Press **Y** to reselect the components or Enter to continue

Step 3 Press **Y** to reselect the components or **Enter** to continue the installation.

The License message appears prompting you to enter the License information.



Note

If you have installed LMS 3.0 with a purchase license, you will not be prompted for license information. You can directly upgrade to LMS 3.1

Step 4 Enter **L** and specify the License file location.

You need to specify the License information only if you are installing either RME, DFM, IPM CM or HUM. You will not encounter this message while installing other applications.

Based on size of the backed-up data, the time required to build the CiscoWorks database is calculated and the following message appears:

```
Rebuilding databases in CiscoWorks may take approximately X minutes. Do you want to
upgrade the product now? (y/n) [y]:
```

In the above message, *X* is the time calculated to build the database.

Entering **n** terminates the installation.

Step 5 Enter **y** to continue with the installation.

For HUM:

- If you have installed HUM 1.0 with a purchase license, you can directly upgrade to HUM 1.1. You will not be prompted for license information. Skip Step 5.
- If HUM 1.1 is directly installed, a separate licensing screen appears as given in Step 5.

The evaluation copy of HUM is packaged with LMS 3.1 and you need to purchase a separate license to use HUM.

Step 6 Enter any of the following:

- **L** and provide the License file location.
- **E** to opt for an evaluation mode. In this mode, you can provide license information later to fully enable the product.
- **Q** to quit the installation.

If you specify the license file for HUM, the following message appears:

```
You have opted to install the licensed version of CiscoWorks HUM 1.1. To use this
application, ensure that you have a licensed version of LMS 3.1.
```

The above message implies that you can install the licensed version of HUM only over the licensed version of LMS.

If you choose the evaluation option, the following message appears:

```
You have opted to evaluate CiscoWorks HUM 1.1. This is valid only for 90 days. If you
provide the licensing information later, ensure that you have installed a licensed
version of LMS 3.1, to continue using the application.
```

The installation program calculates the minimum disk space, RAM and SWAP space required to install the product and the space required to rebuild the database.

- If the disk space is sufficient, the following message appears:

```
Sufficient disk space.
```

- If the drive does not have enough space, an error message appears and the installation exits.

The Installation program provides a tool called Performance Tuning Tool (PTT), which fine-tunes RME to utilize the system resources better. If the CiscoWorks server has a dual CPU with 4 GB RAM, the following message appears:

```
Do you want to tune RME to better utilize the available System resources, and improve
performance?
```

```
Select Yes, to tune the performance parameters of RME towards the end of installation.
Select No, to continue running RME using the existing default parameters. If you select
No, you can tune the parameters later by running rmeptt CLI utility. See the "Performance
Tuning Tool" section of RME user Guide for Details.<y/n> [n]:
```

Step 7 Enter:

- **y** to tune RME for better utilization of System Resources
- Or
- **n** to continue with the installation.

If you select **y**, RME is fine tuned at the end of the installation.

For CiscoWorks Assistant alone, a random password is generated and the following message appears:

```
Do you want to see the passwords that were entered/randomly generated? If yes, please
remember that passwords are security sensitive data and hence make sure they are kept
secure.? (y/n) [y]:
```

Step 8 Enter **y**.

The following message appears:

```
WARNING: Exiting installation beyond this point might result in system instability.
Do you want to continue the installation? (y/n) [y]:
```

Step 9 Enter **y**.

Installation now proceeds. At the end of installation, the following messages appear if you installed the respective applications:

```
WARNING: To ensure that you retain the latest device support for RME,
WARNING: please install the latest Device Packages from Cisco.com@
WARNING: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme
WARNING: Please refer to the Installing and Getting Started with CiscoWorks LAN Management
Solution 3.1 guide for details.
```

The above message appears only if you have installed RME.

WARNING: To ensure that you retain the latest device support for CM,
WARNING: please install the latest Device Packages from Cisco.com @
WARNING: <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-campus>
WARNING: Please refer to the Installing and Getting Started with CiscoWorks LAN Management Solution 3.1 guide for details.

The above message appears only if you have installed CM.

WARNING: To ensure that you have up-to-date device support,
WARNING: install the latest Service Pack (SP) from Cisco.com, at
WARNING: <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.
WARNING: For installation details, refer to the Installing and Getting Started with CiscoWorks LAN Management Solution 3.1 guide.

The above message appears only if you have installed DFM.

The installation completes without displaying more questions and the system prompt appears. It takes about an hour to complete the installation.

The following messages appear at the end of the installation:

Software Installation Tool Completed
Possible Warnings/Errors Encountered

The warning and error messages that appear after these messages do not hinder the installation. They only indicate that you need to take corrective actions after the installation has completed.

Your Solaris machine has the selected applications of LMS 3.1 installed successfully.

**Note**

On Solaris 10 if you have selected to install DFM, a warning message may appear prompting you to reboot the machine at the end of installation. If the settings required by DFM are already available, the message may not appear.

**Note**

If cluster patches are installed for Solaris 10, you must reboot your system after installing LMS.

To prepare the client system for use, see [System and Browser Requirements for Server and Client](#).

For troubleshooting information, see [Checking Processes After Installation](#) and [Understanding Installation Error Messages](#).

Local Upgrade to LMS 3.1 on Solaris — Custom

To perform a local upgrade to LMS 3.1 on a Solaris machine, using the Custom option:

Step 1 Go to the command prompt and select either:

- **2** and **Enter** to proceed with the installation after you select the Custom mode.

Or

- **Q** to quit the installation.

If you press **Enter** a list of the applications appears.

```

1) Common Services 3.2
2) LMS Portal 1.1
3) CiscoWorks Assistant 1.1
4) CiscoView 6.1.8
5) Integration Utility 1.8
6) Resource Manager Essentials 4.2
7) Campus Manager 5.1
8) Device Fault Manager HPOV-NetView adapters 3.1
9) Device Fault Manager 3.1
10) Internetwork Performance Monitor 4.1
11) All of the above
-----Add-on Applications-----
12)Health and Utilization Monitor 1.1
-----

```

You can select and install one or more applications. By default the applications you installed in the earlier version of LMS appear as selected for upgrade.

Step 2 Enter the number corresponding to the option you have chosen or **Q** to quit.

Make sure you have sufficient disk space. For disk space requirements, see [System and Browser Requirements for Server and Client](#).

You must select Common Services 3.2, LMS Portal 1.1 and CiscoWorks Assistant 1.1 applications before selecting any other applications.

Integration Utility 1.8 can be installed independently. It does not depend on Common Services 3.2 or LMS Portal 1.1 or any application for installation.

You cannot install or reinstall both DFM 3.1 and DFM 3.1 HPOV- NetView Adapters at the same time. If you do, you will be prompted by an information message to reselect the applications.

You can select more than one application.

To do this enter the numbers of the options, separated by commas. To quit enter **Q**.

After you select the applications, the following message is displayed:

```
Press Y to reselect the components or Enter to continue
```

Step 3 Press **Y** to reselect the components or **Enter** to continue the installation.

The License prompt appears where you need to provide the suitable license information.

**Note**

If you have installed LMS 3.0 with a purchase license, you will not be prompted for license information. You can directly upgrade to LMS 3.1

Step 4 Enter **L** and specify the License file location.

You need to specify the License information only if you are installing either RME, DFM, IPM CM or HUM. You will not encounter this message while installing other applications.

After that, the Database Password prompt appears.

Step 5 Enter the Database password.

This password must begin with an alphabet and should be less than 15 characters. It will be used internally by the product.

Based on size of the backed-up data, the time required to build the CiscoWorks database is calculated and the following message appears:

```
Rebuilding databases in CiscoWorks may take approximately X minutes. Do you want to
upgrade the product now? (y/n) [y]:
```

In the above message, *X* is the time calculated to build the database.

Entering **n** terminates the installation.

Step 6 Enter **y** to continue with the installation.

For more information on passwords, see [Password Information](#).

You have to provide the license information for HUM as follows:

- If you have installed HUM 1.0 with a purchase license, you can directly upgrade to HUM 1.1. You will not be prompted for license information. Skip Step 5.
- If HUM 1.1 is directly installed, a separate licensing screen appears as given in Step 6.

The evaluation copy of HUM is packaged with LMS 3.1 and you need to purchase a separate license to use HUM.

Step 7 Enter any of the following:

- **L** and provide the License file location.
- **E** to opt for an evaluation mode. In this mode, you can provide license information later to fully enable the product.
- **Q** to quit the installation.

If you specify the license file for HUM, the following message appears:

```
You have opted to install the licensed version of CiscoWorks HUM 1.1. To use this
application, ensure that you have a licensed version of LMS 3.1.
```

The above message implies that you can install the licensed version of HUM only over the licensed version of LMS.

If you choose the evaluation option, the following message appears:

```
You have opted to evaluate CiscoWorks HUM 1.1. This is valid only for 90 days. If you
provide the licensing information later, ensure that you have installed a licensed
version of LMS 3.1, to continue using the application.
```

The installation program calculates the minimum disk space, RAM and SWAP space required to install the product and the space required to rebuild the database.

- If the disk space is sufficient, the following message appears:
Sufficient disk space.
- If the drive does not have enough space, an error message appears and the installation exits.

Step 8 Enter the CiscoWorks Admin password and confirm it.

For more information on passwords, see [Password Information](#).

Step 9 Enter the guest password and confirm it.

For more information on passwords, see [Password Information](#).

Step 10 Enter the System Identity Account password and confirm it.

In a multi-server environment, you must configure all systems part of your multi-server setup with the same System Identity Account password.

For more information on passwords, see [Password Information](#).

The SSL certificate message appears.

Do you want to preserve the existing Apache Certificate? (y/n): [y]

Step 11 Press **Y** to proceed.

Step 12 Enter the SMTP server name. For more information, see [License Information](#)

Step 13 Enter the country code, state, city, company, organization, administrator's e-mail address, and host name for HTTPS.

Only the Host name is mandatory. Other fields are optional. Press **Enter** to skip other fields.

Step 14 Enter either:

- **N** not to integrate with a third-party NMS after installation. This completes the installation faster. It also avoids errors that may be caused by third party integration.
- **Y** to integrate with a third-party NMS during installation.

If you select **Y**:

a. Select any of the following:

- The adapter from the list of available adapters.
- **Other** to choose an adapter that is not listed (you are prompted to enter the path name of the adapter).
- **None** to integrate after the installation is complete.

If you select **None**, go to [Step 14](#).

Many third-party products allow you to launch CiscoWorks applications from within the third-party product. The CiscoWorks applications are launched in a web browser.

b. Enter the full pathname for the web browser.

A message prompts you to enable download updates to NMIDB (Network Management Integration Data Bundle) directly from Cisco.com.

c. Select either:

- **N** to disable future updates from Cisco.com.
- **Y** to enable future updates from Cisco.com.

If you select **N**, go to [Step 14](#).

- d. Enter your Cisco.com user ID and password.

You must have Cisco.com login privileges. If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the standard Cisco.com web site.

The installation program checks dependencies and system requirements and copies the files to the run time.

The Installation program provides a tool called Performance Tuning Tool (PTT), which fine-tunes RME to utilize the system resources better. If the CiscoWorks server has a dual CPU with 4 GB RAM, the following message appears:

```
Do you want to tune RME to better utilize the available System resources, and improve
performance?
```

```
Select Yes, to tune the performance parameters of RME towards the end of installation.
Select No, to continue running RME using the existing default parameters. If you select
No, you can tune the parameters later by running rmeptt CLI utility. See the "Performance
Tuning Tool" section of RME user Guide for Details.<y/n> [n]:
```

Step 15 Enter:

- y to tune RME for better utilization of System Resources

Or

- n to continue with the installation.

If you select y, RME is fine tuned at the end of the installation.

A message appears:

```
Do you want to see the passwords that were entered/randomly generated? (y/n) [n]
```

The Device Fault Manager uses a data transport protocol that requires authentication for server-to-server communication. You can retain the existing username and password for securing this interface.

Step 16 Enter y.

A message appears:

```
Exiting installation beyond this point might result in system instability.
```

```
Do you want to continue the installation? (y/n) [y]
```

Installation now proceeds. At the end of installation, the following messages appear:

```
WARNING: To ensure that you retain the latest device support for RME,
```

```
WARNING: please install the latest Device Packages from Cisco.com @
```

```
WARNING: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme
```

```
WARNING: Please refer to the Installing and Getting Started with CiscoWorks LAN Management
Solution 3.1 guide for details.
```

The above message appears only if you have installed RME.

```
WARNING: To ensure that you retain the latest device support for CM,
```

```
WARNING: please install the latest Device Packages from Cisco.com @
```

```
WARNING: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-campus
```

```
WARNING: Please refer to the Installing and Getting Started with CiscoWorks LAN Management
Solution 3.1 guide for details.
```

The above message appears only if you have installed CM.

```
WARNING: To ensure that you have up-to-date device support,
```

```
WARNING: install the latest Service Pack (SP) from Cisco.com, at
```

```
WARNING: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm.
```

```
WARNING: For installation details, refer to the Installing and Getting Started with
CiscoWorks LAN Management Solution 3.1 guide.
```

The above message appears only if you have installed DFM.

The installation completes without displaying more questions and the system prompt appears.

It takes approximately an hour to complete the installation.

The following messages appear at the end of the installation:

```
Software Installation Tool Completed
```

```
Possible Warnings/Errors Encountered
```

The warning and error messages that appear after these messages do not hinder the installation. They only indicate that you need to take corrective actions after the installation has completed.

Your Solaris machine has the selected applications of LMS 3.1 installed successfully.

**Note**

On Solaris 10 if you have selected to install DFM, a warning message may appear prompting you to reboot the machine at the end of installation. If the settings required by DFM are already available, the message may not appear.

**Note**

If cluster patches are installed for Solaris 10, you must reboot your system after installing LMS.

To prepare the client system for use, see [System and Browser Requirements for Server and Client](#).

For troubleshooting information, see [Checking Processes After Installation](#) and [Understanding Installation Error Messages](#).

Remote Upgrade to LMS 3.1 on Solaris

To upgrade from the previous versions of LMS to LMS 3.1 on a different Solaris machine:

- Step 1** Login to the machine where the previous version of LMS is installed.
- Step 2** Take a backup of the LMS data.
- Step 3** Login to the machine where LMS 3.1 is to be installed.
- Step 4** Follow the install procedure using Typical or Custom to install LMS 3.1. See [Installing LMS 3.1 on Solaris - New](#).
- Step 5** Migrate the data to LMS 3.1.

To migrate and restore the LMS data, follow the procedure in the *Data Migration Guide for LAN Management Solution 3.1*.

The *Data Migration Guide for LAN Management Solution 3.1* is available at this location:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html

Notes for Remote Upgrade

The list of applications in the backed-up machine should exactly match the list of applications in the machine where it is restored. If not, the behavior of the applications after upgrade will be unpredictable.

For example:

- You have backed up data for:
 - CS 3.1
 - RME 4.1
 - CM5.0
- You restore it in a machine that has:
 - CS 3.2
 - RME 4.2
 - CM 5. 1
 - DFM 3.1
 - HUM 1.1

For the above scenario, the behavior of the applications after upgrade will be unpredictable. For more details on backing up and restoring data, see the *Data Migration Guide for LAN Management Solution 3.1*.

Local Upgrade to LMS 3.1 on Windows

To upgrade to LMS 3.1 on the same Windows machine, you can select the relevant option from the following:

- Customers having LMS 2.5 or LMS 2.5.1, must first install LMS 2.6, available from Cisco.com and then proceed to upgrade LMS 3.1 from the DVD.

The LMS 2.6 is available at the location:

<http://www.cisco.com/cgi-bin/tablebuild.pl/lms26>.

For install instructions, see the Readmes at:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html.

- Customers upgrading from LMS 2.6, LMS 2.6 SP1, LMS 3.0 and LMS 3.0 December 2007 update can directly upgrade to LMS 3.1.

**Note**

We recommend that you take a backup of your data before you start the upgrade.

To upgrade to LMS 3.1 on the same Windows machine:

Step 1 Login as administrator to the machine where the previous version of LMS is already installed.

- a. Insert the LMS 3.1 DVD.
- b. Double-click on the autorun.exe or setup.exe file.

The CiscoWorks LAN Management Solution 3.1 Applications window appears.

- c. Click **Install** to continue.

While installing from the network drive, the Installing from Network Drive window appears.

Installation from network drive will be slower than installing from the local drive.

Step 2 Click **Yes** to proceed or **No** to exit installation.

If the WMI service is running, the following message appears when installation starts:

Windows Management Instrumentation (WMI) is running. This locks processes and impedes installation. To avoid WMI conflicts, this Setup program will stop and immediately restart the WMI service.

Do you want to proceed?

Click Yes to proceed with this installation. Click No to exit installation.

Step 3 Click **Yes** to proceed.

The IIS detection message appears.

When Internet Information Services (IIS) is detected on your system and if you have continued the installation without IIS services, you cannot use the port number 443 for HTTPS. Instead, you must use the port numbers ranging from 1026 to 65535 for HTTPS to avoid this conflict.

Step 4 Click **Yes** or **No** to continue.

When you upgrade from a LMS 3.0 machine, that has the evaluation version of HUM installed, the following message appears:

You have opted to upgrade the LMS version from 3.0 to 3.1. If you have an evaluation version of HUM, ensure that you uninstall the evaluation version before upgrading. If you have a valid license for HUM, ensure that you apply the license before upgrading.

Do the following:

- a. Uninstall the evaluation version of HUM. For details, see [Uninstalling LMS 3.1 on Windows](#)
- b. Repeat [Step 1](#).

OR

Apply the license for HUM and proceed with the installation.

Installation checks for the Regional Settings. They have to be set either as US English or Japanese.

If the Primary settings point to an unsupported locale, the following warning message appears:

You are trying to install CiscoWorks on an unsupported locale. CiscoWorks supports only US English or Japanese languages. Please reinstall your Operating System with a supported locale and change the Regional Settings to either of these languages.

Click Yes to continue installing CiscoWorks or No to exit.

Step 5 Click:

- **Yes** to continue the installation
- **No** to terminate the installation.

You can install LMS after re-installing the Operating System with the supported locale.

If the Active settings point to an unsupported locale, the following warning message appears:

You are trying to install CiscoWorks on an unsupported locale. CiscoWorks supports only US English or Japanese languages. Please change the Regional Settings to either of these languages.

Click Yes to continue installing CiscoWorks or No to exit.

Step 6 Click:

- **Yes** to continue the installation
- **No** to terminate the installation.

You can install LMS after correcting the Active regional settings in **Control Panel > Regional and Language Options > Regional Options**.

The Welcome window appears.

Step 7 Click **Next** to continue.

The Software License Agreement window appears. You must accept this agreement to install CiscoWorks LMS 3.1.

Step 8 Click **Accept** to continue.

If you are trying to install on an unsupported platform, the following error message appears:

```
You cannot install CiscoWorks LMS 3.1 application(s) on an unsupported operating system
or when Terminal Services is running on the supported Windows 2003 Server Standard
Edition, Windows 2003 Server Enterprise Edition, and Windows 2003 R2 Server platforms
The setup program will exit when you click OK
```

You must either upgrade the operating system on the server to a supported version or install LMS 3.1 application(s) on another server that runs a supported operating system.

You cannot install LMS 3.1 on Windows 2000 server platform. You need to upgrade to Windows 2003 operating system and then continue with installation. If not, installation will terminate.

When you have the recommended platform, the installation continues.

If you are trying to install CiscoWorks Common Services on a Primary Domain Controller or Backup Domain Controller, installation terminates after showing the following error message:

```
You are attempting to install CiscoWorks Common Services 3.2 on a server that is
configured as a Primary Domain Controller or a Backup Domain Controller (PDC/BDC).
```

Install CiscoWorks Common Services 3.2 on another server not configured as PDC / BDC.

The Setup Type dialog box appears.

Step 9 Select one of the following:

You can upgrade install LMS 3.1 using either the Typical or Custom mode:

- **Typical** to select the components and install the selected components in the default location (*System Drive\Program Files\CSCOpX*). This is the default installation mode. (See the [Local Upgrade to LMS 3.1 on Windows — Typical](#) section.)
- **Custom** to select the components, customize the settings, and to specify the location. (See the [Local Upgrade to LMS 3.1 on Windows — Custom](#) section.)

Local Upgrade to LMS 3.1 on Windows — Typical

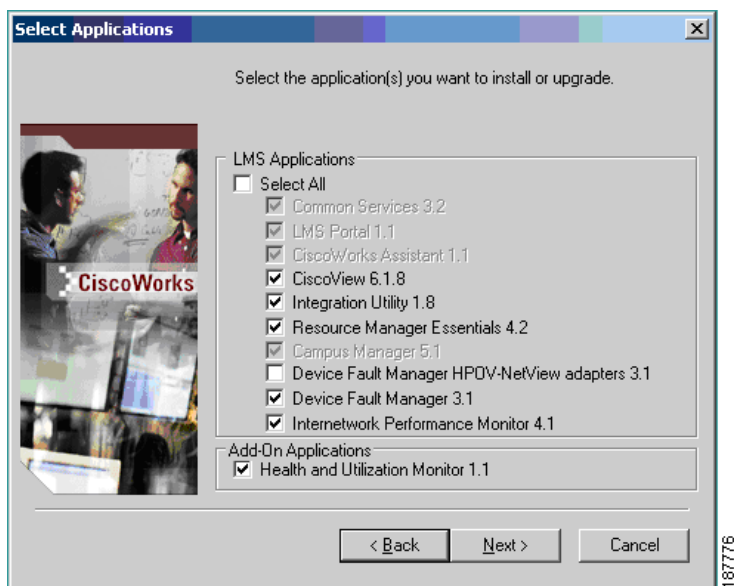
To upgrade to LMS 3.1 on the same Windows machine, using the Typical option:

Step 1 Click **Next** to continue after you select the Typical installation mode.

The Backup Data dialog box appears.

Step 2 Select a suitable location for backup and click **Next**.

The Select Applications dialog box appears as given in [Figure 4-6](#).

Figure 4-6 *Select Applications Dialog Box in Upgrade Scenario*

The existing applications in the earlier versions of LMS will get selected and upgraded to its latest version by default when you install LMS 3.1.

You can also now select to install or reinstall any other application of LMS 3.1.

You cannot install or reinstall both DFM 3.1 and DFM 3.1 HPOV- NetView Adapters at the same time. If you do, you will be prompted by an information message to select only one of them.

Step 3 Click **Next** to continue.

The Licensing Information dialog box appears for LMS 3.1.

**Note**

If you have installed LMS 3.0 with a purchase license, then this licensing screen does not appear. You can directly upgrade to LMS 3.1

Step 4 Specify the License File Location.

You need to specify the License information only if you are installing either RME, DFM, IPM CM or HUM. You will not encounter this message while installing other applications.

For HUM:

- If you have installed HUM 1.0 with a purchase license, you can directly upgrade to HUM 1.1. A separate licensing screen does not appear. Skip Step 6 and Step 7.
- If HUM 1.1 is directly installed, a separate licensing screen appears.

The evaluation copy of HUM is packaged with LMS 3.1 and you need to purchase a separate license to use HUM.

Step 5 Specify the License File Location or select the Evaluation option.

- If you specify the license file for HUM, the following message appears:

You have opted to install the licensed version of CiscoWorks HUM 1.1. To use this application, ensure that you have a licensed version of LMS 3.1.

The above message implies that you can install the licensed version of HUM only over the licensed version of LMS.

- If you choose the Evaluation option, the following message appears:

You have opted to evaluate CiscoWorks HUM 1.1. This is valid only for 90 days. If you provide the licensing information later, ensure that you have installed a licensed version of LMS 3.1, to continue using the application.

Step 6 Click **OK**.

Based on size of the backed-up data, the time required to build the CiscoWorks database is calculated and the following message appears:

Rebuilding databases in CiscoWorks may take approximately *X* minutes. Do you want to upgrade the product now?

Click **Yes** to upgrade the product now or **No** to upgrade later.

In the message, *X* is the time taken to rebuild the database.

Clicking **No** terminates the installation.

Step 7 Click **Yes** to continue with the installation.

The System Requirements dialog box appears.

The installation program calculates the minimum disk space, RAM and SWAP space required to install the product and the space required to rebuild the database.

The Web Server dialog box appears.

Step 8 Enter HTTPS port, server administrator e-mail address, and the SMTP server name.

The default HTTPS port number is 443. The SMTP server name is used by other CiscoWorks applications. The HTTPS port and SMTP server name are mandatory.



Note

When IIS is detected on your system, to avoid any conflict with HTTPS, use port numbers ranging from 1026 to 65535.

Step 9 Click **Next**.

The Installation program provides a tool called Performance Tuning Tool (PTT), which fine-tunes RME to utilize the system resources better. If the CiscoWorks server has a dual CPU with 4 GB RAM, the following message appears:

Do you want to tune RME to better utilize the available System resources, and improve performance?

Select **Yes**, to tune the performance parameters of RME towards the end of installation. Select **No**, to continue running RME using the existing default parameters. If you select **No**, you can tune the parameters later by running `rmeptt` CLI utility. See the "Performance Tuning Tool" section of RME user Guide for Details.

Step 10 Click:

- **Yes** to tune RME for better utilization of System Resources

Or

- **No** to continue with the installation.

If you select **Yes**, RME is fine tuned at the end of the installation.

The Summary window appears with the updates that will be installed and the settings for the installation.

Step 11 Click **Next**.

The Stop All Programs dialog box appears with the list of files currently being used by other processes.

Step 12 Click **Retry** to verify.

Installation continues.

At the end of installation, based on the applications you have selected to install or reinstall, warning messages appear. These messages prompt you to install the latest device latest updates as indicated in [Figure 4-4](#).

Step 13 Click **OK** and proceed to complete the installation.

Information about the various LMS applications, their features and benefits are displayed during installation.

The Restart dialog box appears after the installation is complete.

You must restart your machine after you have installed LMS 3.1.

Step 14 Select **Yes, I want to restart my computer now**.

Step 15 Click **Finish**.

To prepare the client system for use, see [System and Browser Requirements for Server and Client](#).

For troubleshooting information, see [Checking Processes After Installation](#) and [Understanding Installation Error Messages](#).

Local Upgrade to LMS 3.1 on Windows — Custom

To upgrade to LMS 3.1 on the same Windows machine, using the Custom option:

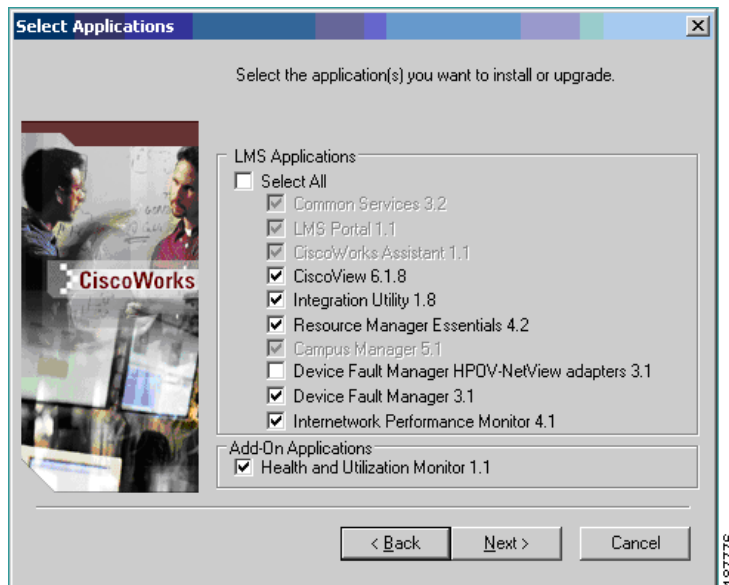
Step 1 Click **Next** to continue after you select the Custom installation mode.

The Backup Data dialog box appears.

Step 2 Select a suitable location for backup.

Step 3 Click **Next**.

The Select Applications dialog box appears as given in [Figure 4-7](#):

Figure 4-7 Select Applications Dialog Box in Upgrade Scenario

The existing applications in the earlier versions of LMS will get selected and upgraded to its latest version by default when you install LMS 3.1.

You can also now select to install or reinstall any other application of LMS 3.1.

You cannot install or reinstall both DFM 3.1 and DFM 3.1 HPOV- NetView Adapters at the same time. If you do, you will be prompted by an information message to select only one of them.

Step 4 Click **Next** to continue.

The Licensing Information dialog box appears for LMS 3.1.

**Note**

If you have installed LMS 3.0 with a purchase license, then this licensing screen does not appear. You can directly upgrade to LMS 3.1

Step 5 Specify the License File Location.

You need to specify the License information only if you are installing either RME, DFM, IPM CM or HUM. You will not encounter this message while installing other applications.

For HUM:

- If you have installed HUM 1.0 with a purchase license, you can directly upgrade to HUM 1.1. A separate licensing screen does not appear. Skip Step 6 and Step 7.
- If HUM 1.1 is directly installed, a separate licensing screen appears.

The Evaluation copy of HUM is packaged with LMS 3.1 and you need to purchase a separate license to use HUM.

Step 6 Specify the License File Location or select the Evaluation option.

- If you specify the license file for HUM, the following message appears:

You have opted to install the licensed version of CiscoWorks HUM 1.1. To use this application, ensure that you have a licensed version of LMS 3.1.

The above message implies that you can install the licensed version of HUM only over the licensed version of LMS.

- If you choose the Evaluation option, the following message appears:

You have opted to evaluate CiscoWorks HUM 1.1. This is valid only for 90 days. If you provide the licensing information later, ensure that you have installed a licensed version of LMS 3.1, to continue using the application.

Step 7 Click **OK**.

Based on size of the backed-up data, the time required to build the CiscoWorks database is calculated and the following message appears:

Rebuilding databases in CiscoWorks may take approximately X minutes. Do you want to upgrade the product now?

Click Yes to upgrade the product now or No to upgrade later.

In the message, X is the time taken to rebuild the database.

Clicking **No** terminates the installation.

Step 8 Click **Yes** to continue with the installation.

The System Requirements dialog box appears.

The installation program calculates the minimum disk space, RAM and SWAP space required to install the product and the space required to rebuild the database.

Step 9 Click **Next**.

The Change Admin and Guest Password box appears.

Step 10 Enter user admin and user guest passwords and confirm them.

For more information on passwords, see [Password Information](#).

Step 11 Click **Next** to continue installation.

The Change System Identity Account password dialog box appears.

Step 12 Enter the System Identity Account password and confirm it.

In a multi-server environment, you must configure all systems part of your multi-server setup with the same System Identity Account password.

For more information on passwords, see [Password Information](#).

Step 13 Click **Next**.

The Change casuser Password dialog box appears.

Casuser is the user who administers and maintains CiscoWorks Server, without administrative privileges.

If you do not enter a password, the installation program generates a random password and adds the new user casuser and the new group casusers to the system.

Step 14 Click **Next** to continue.

The Database Password dialog box appears.

For more information on passwords, see [Password Information](#).

Step 15 Click **Next** to continue installation.

The Web Server dialog box appears.

Step 16 Enter HTTPS port, server administrator e-mail address, and the SMTP server name.

The default HTTPS port number is 443. The SMTP server name is used by other CiscoWorks applications. The HTTPS port and SMTP server name are mandatory.



Note

When IIS is detected on your system, to avoid any conflict with HTTPS, use port numbers ranging from 1026 to 65535.

Step 17 Click **Next** to continue installation.

The Self-Signed Certificate dialog box appears. The webserver uses the Self-Signed certificate while operating in secure mode.

Step 18 Enter the country code, state, city, company, organization, and host name for HTTPS.

The host name is mandatory.

Step 19 Click **Next** to continue installation.

If you want to create a shortcut to CiscoWorks on your desktop, select the check box.

Step 20 Click **Next**.

The Installation program provides a tool called Performance Tuning Tool (PTT), which fine-tunes RME to utilize the system resources better. If the CiscoWorks server has a dual CPU with 4 GB RAM, the following message appears:

Do you want to tune RME to better utilize the available System resources, and improve performance?

Select **Yes**, to tune the performance parameters of RME towards the end of installation. Select **No**, to continue running RME using the existing default parameters. If you select **No**, you can tune the parameters later by running `rmeptt` CLI utility. See the "Performance Tuning Tool" section of RME user Guide for Details.

Step 21 Click:

- **Yes** to tune RME for better utilization of System Resources
- Or
- **No** to continue with the installation.

If you select **Yes**, RME is fine tuned at the end of the installation.

The Summary window appears with the updates that will be installed and the settings for the installation.

Step 22 Click **Next**.

The Stop All Programs dialog box appears with the list of files currently being used by other processes running.

Step 23 Click **Retry** to verify and proceed.

Installation continues.

At the end of installation, based on the applications you have selected to install or reinstall, warning messages appear. These messages prompt you to install the latest device latest updates as indicated in [Figure 4-4](#).

Step 24 Click **OK** and proceed to complete the installation.

Information about the various LMS applications, their features and benefits are displayed during installation.

The Restart dialog box appears after the installation is complete.

You must restart your machine after you have installed LMS 3.1.

Step 25 Select **Yes, I want to restart my computer now**.

Step 26 Click **Finish**.

To prepare the client system for use, see [System and Browser Requirements for Server and Client](#).

For troubleshooting information, see [Checking Processes After Installation](#) and [Understanding Installation Error Messages](#).

Remote Upgrade to LMS 3.1 on Windows

To remote upgrade from the previous version of LMS to LMS 3.1 on a different Windows machine:

Step 1 Log into the machine where the previous version of LMS is installed.

Step 2 Take a backup of the LMS data.

Step 3 Log into the machine where LMS 3.1 is to be installed.

Step 4 Follow the install procedure using Typical or Custom to install LMS 3.1. See [Installing LMS 3.1 on Windows - New](#).

Step 5 Migrate the data to LMS 3.1.

To migrate and restore the LMS data follow the procedure in the *Data Migration Guide for LAN Management Solution 3.1*.

The *Data Migration Guide for LAN Management Solution 3.1* is available at this location:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html

Notes for Remote Upgrade

The list of applications in the backed-up machine should exactly match the list of applications in the machine where it is restored. If that is not the case, behavior of the applications after upgrade will be unpredictable.

For example:

- You have backed up data for:
 - CS 3.1
 - RME 4.1
 - CM5.0

- You restore it in a machine that has:
 - CS 3.2
 - RME 4.2
 - CM 5.1
 - DFM 3.1
 - HUM 1.1

For the above scenario, behavior of the applications after upgrade will be unpredictable. For more details on backing up and restoring the data, see the *Data Migration Guide for LAN Management Solution 3.1*.

Verifying the Installation

You can verify LMS 3.1 installation by following either of these procedures.

Procedure 1

You can verify LMS 3.1 installation using either of these methods:

- Enter the command **pdshow** from *NMSROOT/bin*.
Where, *NMSROOT* is the CiscoWorks installation directory (by default, SystemDrive:\Program Files\CSCOpX and *SystemDrive* is the Windows operating system installed directory and for Solaris it is /opt/CSCOpX).
- Select **Common Services > Server > Admin > Processes** on the CiscoWorks Home page, to see the various processes and their status.

The services that should be displayed after installation are listed below. For details on the various process statuses, refer to the *User Guide for Common Services 3.2*:

Application Name	Services/Processes	
Common Services 3.2	<ul style="list-style-type: none"> Apache CmfDbEngine CmfDbMonitor CMFOGSServer CSDiscovery CSRegistryServer DCRServer diskWatcher EDS EDS-GCF ESS EssMonitor FDRewinder (Only on Solaris) jrm LicenseServer NameServer NameServiceMonitor Tomcat TomcatMonitor 	
Campus Manager 5.1	<ul style="list-style-type: none"> ANIServer ANIDbEngine CampusOGSServer UTManager UTLITE UTMajorAcquisition MACUHIC WlseUHIC 	

Application Name	Services/Processes	
Resource Manager Essentials 4.2	<ul style="list-style-type: none"> • ChangeAudit • ConfigMgmtServer • CTMJrmServer • EssentialsDM • ICServer 	<ul style="list-style-type: none"> • RMEDbEngine • RMEOGSServer • SyslogAnalyzer • SyslogCollector
Device Fault Manager 3.1	<ul style="list-style-type: none"> • AdapterServer • AdapterServer1 • DataPurge • DfmServer • DfmServer1 • DFMLogServer • DFMCTMStartup • DfmBroker • DFMMultiProcLogger • DFMOGSServer • EPMServer • EPMDbEngine • FHPurgeTask 	<ul style="list-style-type: none"> • FHDbEngine • FHServer • Interactor • Interactor1 • InventoryCollector • InventoryCollector1 • INVDbEngine • NOSServer • PMServer • PTMServer • TISServer
Internetwork Performance Monitor 4.1	<ul style="list-style-type: none"> • IPMProcess • IpmDbEngine 	<ul style="list-style-type: none"> • IPMOGSServer
CiscoWorks Assistant 1.1	<ul style="list-style-type: none"> • OpsxmlDbEngine • OpsXMLRuntime 	<ul style="list-style-type: none"> • ProcSysBus
Health and Utilization Monitor 1.1	<ul style="list-style-type: none"> • UPMDbEngine • UPMPProcess 	<ul style="list-style-type: none"> • UPMDbMonitor

Procedure 2

To verify from the CiscoWorks Home Page main screen:

Step 1 Select **Common Services > Server > Home Page Admin > Application Registration**.

The Application Registration Status page appears.

Step 2 Check the Registered Applications table.

If LMS 3.1 is upgraded successfully, the following application versions will be listed:

- CiscoView 6.1
- RME 4.2
- Campus Manager 5.1
- Device Fault Manager 3.1

- Internetwork Performance Monitor 4.1
- Health and Utilization Monitor 1.0

Application Registration Status page displays only the major version of the product. See the Software Updates page on Common Services to know the version with patch levels for all applications.

Procedure 3

You can also verify the installation using Software Center. To verify the installation, go to **Common Services > Software Center > Software Update** and the Software Updates page appears. You can verify the installation using the Products installed dialog box.

For information on installing User Tracking Utility on a Windows client, see [User Tracking Utility](#).

For information on installing the Remote Syslog Collector, see [Installing the Remote Syslog Collector](#).

Uninstalling LMS 3.1

This section contains:

- [Before You Begin Uninstallation](#)
- [Uninstalling LMS 3.1 on Solaris](#)
- [Uninstalling LMS 3.1 on Windows](#)

Before You Begin Uninstallation

The following are some precautionary notes on uninstallation that you must read:

- CiscoWorks Common Services 3.2, CiscoWorks LMS Portal 1.1 and CiscoWorks Assistant 1.1 must be uninstalled together. If not, you will encounter some error messages.
- As CiscoWorks Common Services 3.2 is required for other applications, it must be uninstalled only at the end. You can also use **Select All** to uninstall all the applications at the same time.
- The uninstall log file will be generated using time stamp with the YYYYMMDD_hhmmss format, for example, C:/CiscoWorks_uninstall_YYYYMMDD_hhmmss.
- The install folder will be removed and the casuser will be removed after uninstallation of Common Services 3.2.

Use the Uninstall option to remove CiscoWorks Common Services files and settings. You must be logged in as administrator to uninstall any application.

You need to uninstall all applications that depend on CiscoWorks before uninstalling CiscoWorks Common Services 3.2.

For example, if you select Common Services without selecting CiscoView, the following message appears on both Windows and Solaris:

```
Cannot uninstall CiscoWorks Common Services.  
It is required for CiscoView.
```

Uninstalling LMS 3.1 on Solaris

To uninstall LMS 3.1 on a Solaris system:

Step 1 Enter the following commands as root to start the uninstall script:

```
# cd /
```

```
# /opt/CSCOpX/bin/uninstall.sh
```

where */opt/CSCOpX* is the default installation directory.

If you have installed applications dependent on Common Services, a list of applications appear.

Enter the number corresponding to the option you have chosen or **q** to quit. You can select more than one component. Enter the number corresponding to the components separated by commas.

When you remove CiscoWorks Common Services (all the CiscoWorks applications), the uninstall script removes changes made to the */etc/services* file. The */etc* directory still contains all system file changes.

The uninstall messages get appended to the */var/tmp/Ciscoworks_uninstall_20060623_102035.log*.

The Uninstallation dialog box appears with the installed components.

Step 2 Enter **Y** to confirm uninstallation of the selected components.

The uninstallation proceeds.

After the uninstall is complete, the following messages appear:

```
All files were deleted successfully.
```

```
Possible Warnings/Errors Encountered
```

The installation program lists the warning and error messages.

Step 3 Check the following files after uninstallation and ensure to perform the following:

- */etc/syslog.conf*

Ensure that the following entry is removed:

```
local0.emerg;local0.alert;local0.crit;local0.err;local0.warning;local0.notice;local0.info;local0.debug /var/adm/CSCOpX/log/dmgted.log.
```

- */etc/services*

Ensure that port assignments for the CiscoWorks applications have been removed.

- */etc/inetd.conf*

Ensure that the CiscoWorks TFTP entry is removed.

Uninstalling LMS 3.1 on Windows

To uninstall LMS 3.1 on a Windows system:

- Step 1** Go to the Windows desktop and select **Start > Programs > CiscoWorks > Uninstall CiscoWorks**.
- If the WMI service is running, the following message appears when uninstallation starts.
- Windows Management Instrumentation (WMI) is running. This locks processes and impedes installation. To avoid WMI conflicts, this Setup program will stop and immediately restart the WMI service.
- Do you want to proceed?
- Click Yes to proceed with this installation. Click No to exit installation.
- Step 2** Click either:
- **Yes** to proceed with this uninstallation.
 - **No** to exit uninstallation.
- The Uninstallation dialog box appears with the installed components.
- Step 3** Select the components you want to remove and click **Next**.
- Or
- Click **Select All** to uninstall all the components and click **Next**.
- The Uninstallation dialog box lists the selected components.
- Step 4** Click either:
- **Next** to continue uninstallation.
- Or
- **Back** to return to the component selection box.
- If you have selected **Uninstall All**, you cannot return to the component selection box using **Back**.
- The uninstallation proceeds and the Uninstallation Complete dialog box appears after uninstallation completes.
- Step 5** Select **Yes, I want to restart my computer now** and click **Finish**.

**Caution**

You must restart your system after the uninstallation is complete. The subsequent installation of other CiscoWorks products may fail if you do not restart your system.

Re-installing LMS 3.1

Re-installation is installing the product over the existing one without performing an uninstallation.

You can re-install LMS 3.1 by running the installation program on the system currently running the product. LMS 3.1 supports new installation and re-installation of applications at the same time.

Re-installation preserves the settings from the previous installation.

LMS applications selected to be re-installed will automatically be installed in the same location, where the previous version was installed.

To reinstall any of the LMS 3.1 applications, follow the similar procedure as detailed in [“Performing New Installation of LMS 3.1” procedure on page 4-2](#).

Notes for Re-installation

- During re-installation, you can choose to enter new passwords or retain the existing ones. For more information on passwords, see [Password Information](#).
- You will be prompted to provide a backup location.
- In Windows, if the WMI service is up and running, the following message appears when installation starts:

```
Windows Management Instrumentation (WMI) is running. This locks processes and impedes
installation. To avoid WMI conflicts, this Setup program will stop and immediately
restart the WMI service.
```

```
Do you want to proceed?
```

```
Click Yes to proceed with this installation. Click No to exit installation.
```

Click **Yes** and proceed with the installation.



CHAPTER 5

Getting Started with LAN Management Solution 3.1

This chapter helps you to get started with CiscoWorks LMS 3.1.

CiscoWorks LMS 3.1 can be installed and deployed on a single server or multiple server environment.

Depending on the type of setup you select, the following sections explain the tasks that you need to perform to work with and understand the product.

The following sections help you to use the LMS 3.1 interface effectively:

- [Before You Start](#)
- [Accessing CiscoWorks Server](#)
- [Logging Into the CiscoWorks Server](#)
- [Understanding the CiscoWorks LMS Portal Home Page](#)
- [Configuring LMS Administration Parameters](#)
- [Setting Up CiscoWorks Server](#)
- [Integrating CiscoWorks Server with ACS](#)
- [Managing Devices in CiscoWorks Server](#)
- [Preparing to Use LMS Applications](#)
- [Performing Maintenance on Your CiscoWorks Server](#)
- [Using CiscoWorks LMS Applications Online Help](#)

Before You Start

Before you start using the LMS 3.1 applications, you must ensure that:

- The network devices that interact with LMS 3.1 are set up correctly.

See Chapter 2, Setting Up Devices on the Network, in the *CiscoWorks LAN Management Solution 3.0 Deployment Guide*:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_white_papers_list.html

See the *CiscoWorks LAN Management Solution 3.0* whitepaper for more information:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_white_papers_list.html

- The license file is installed on your CiscoWorks server.

See the [License Information](#).

Accessing CiscoWorks Server

LMS 3.1 uses port number 1741 to access the CiscoWorks Server in normal (HTTP) mode and port number 443 to access the server in secure (HTTPS) mode by default.

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 LMS applications on the default port, and enter:

`http://server_name:1741`

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

`https://server_name:443`

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

The CiscoWorks Login page appears.

You can also change the default web server port numbers (for HTTP and HTTPS modes) using the *changeport* utility. See *User Guide for CiscoWorks Common Services 3.2* 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 LMS web server, while installing the CiscoWorks applications.

To avoid this conflict, you should change the SSL port number of LMS web server from 443 to some other available port number within the range from 1026 to 65535.

Logging Into the CiscoWorks Server

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

-
- Step 1** Enter the username in the User ID field, and the password in the Password field of the Login page.
- The CiscoWorks server administrator can set the passwords to admin and guest users during installation. Contact the CiscoWorks server administrator if you do not know the password.
- Step 2** Click **Login** or press **Enter**.
- You are now logged into CiscoWorks server.
- The CiscoWorks LMS Portal home page appears.
- See [Understanding the CiscoWorks LMS Portal Home Page](#) for more information.
-

Understanding the CiscoWorks LMS Portal Home Page

The following sections help you to understand the LMS Portal home page and the tasks that you can perform with it:

- [CiscoWorks LMS Portal Home Page](#)
- [Views](#)
- [Portlets](#)
- [Launching LMS Applications](#)
- [Launching LMS Workflow Demos](#)

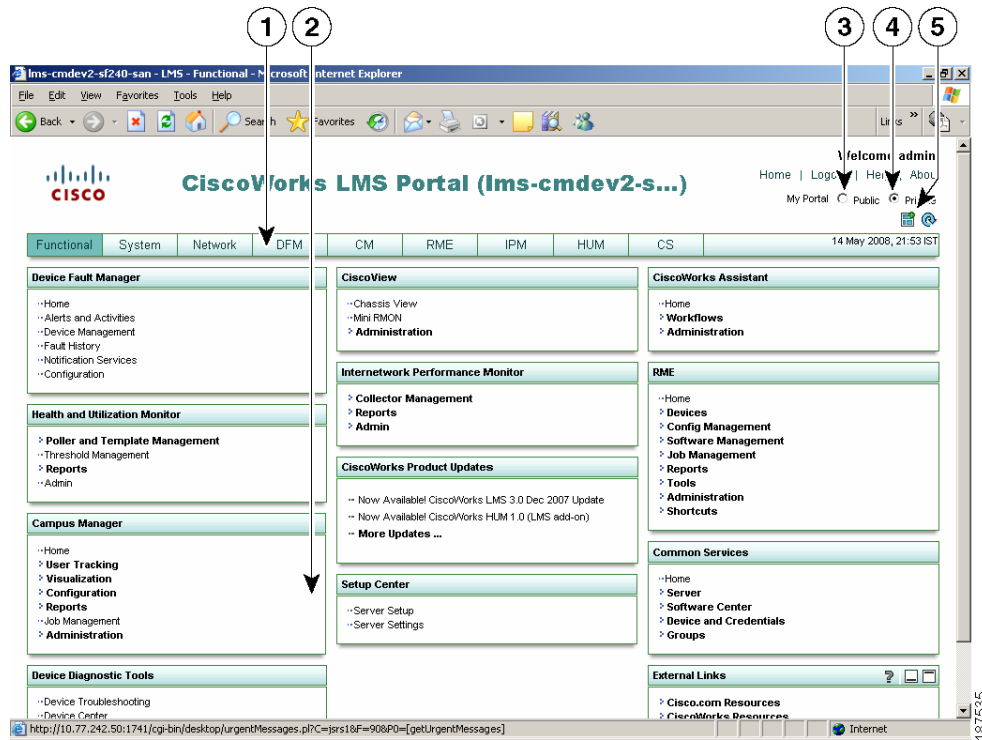
CiscoWorks LMS Portal Home Page

CiscoWorks LMS Portal is the first page that appears when you launch the LMS application. The LMS Portal is designed to give you quick access to important statistics and details of the LMS applications installed on your CiscoWorks server.

CiscoWorks LMS Portal allows you to launch the other LMS applications and provides top-level navigation for frequently-used functions in the LMS applications.

[Figure 5-1](#) displays the CiscoWorks LMS Portal home page.

Figure 5-1 LMS Portal Home Page



1	Views—A page composed to display relevant information, appears as tabs in CiscoWorks LMS Portal.	4	Private Portal—Select the Portal as Private to configure and customize the portlets
2	Portlets—User Interface components that enable you to add information inside a view.	5	Manage Views—Click the Manage View icon to add Views or manage them.
3	Public Portal—Select the Portal as Public to view the portlets added into the Public Portal by the Administrator.		

The LMS Portal application is built using light-weight GUI components. Hence, it does not require any download or installation of any plug-ins for launching the user interface.

See [Table 5-1](#) for a description of each element.

Table 5-1 Portal Window Elements

Element	Function
View	<p>In LMS Portal, view is a page that displays a set of relevant information.</p> <p>LMS Portal comes with four default views such as Functional, System, Network and CS (Common Services).</p> <p>You can also create your own views and add content. The views are displayed as tabs at the top of the page.</p> <p>See Configuring LMS Administration Parameters for more information.</p>
Portlets	<p>Enables you to organize information inside a View. The user interface components are managed and displayed in a view.</p> <p>See Views for more information.</p>
Home	Enables you to view the Portal home page.
Logout	Enables you to exit from the application.
Help	<p>Enables you to view the Online help details. It opens a new window that displays context-sensitive help for the displayed page.</p> <p>The window also contains buttons that take you to the overall help contents, index, and search tool.</p>
About	Enables you to view the details about the licence information of the application. You can click the links displayed in the page to view the valid purchase licence information.
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. By default, LMS portal is a private portal.
Public	<p>LMS Portal can be a Public portal or Private portal. In the Public mode you can view all the portlets added by the Administrator.</p> <p>To select Public Portal, go to CiscoWorks LMS Portal and select Public at the top right corner.</p> <p>You can select the Public portal to view only the portlets added into the Public portal by the administrator.</p>
Manage View	Enables you to add a View and customize a View using View Settings.
Add Portlet	Enables you to add Portlets and select a layout. You cannot add portlets in the Functional view.

Views

Views are the names of installed LMS applications displayed as tabs in CiscoWorks LMS Portal.



Note

The number of Views or tabs vary based on the LMS applications installed on the CiscoWorks server.

Table 5-2 lists the four types of Views.

Table 5-2 Types of Views

View Name	Description
Functional	<p>Contains portlets that help you to launch the applications installed in the CiscoWorks server.</p> <p>This view contains information that was displayed in the CiscoWorks home page for versions of LMS earlier than 3.1.</p> <p>The Functional View contains remotely registered applications. You cannot add or remove portlets, configure or change the look and feel of the portlets in the Functional View.</p> <p>When you log into CiscoWorks for the first time, the Functional View appears as the default View.</p> <p>For subsequent logins, you can set any View as the default view.</p>
Network	Contains network-based portlets from the LMS applications. For instance, if you have installed CM you will get the network view portlets from the CM applications.
System	Contains system-based portlets from CS application.
Common Services	<p>By default CS (Common Services) View and its portlets appear when you launch CiscoWorks LMS Portal.</p> <p>If you have installed RME application (Resource Manager Essentials) an RME View will be displayed along with RME portlets.</p>

For further information on portlets and views, see the Online help or the *User Guide for LMS Portal 1.1*.

Portlets

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

You can add, remove, minimize, maximize, modify the look and feel and also configure the portlets in CiscoWorks LMS Portal. You cannot add or remove portlets in the Functional view.

You can also add portlets from a remote server.

You can save your settings on Portlets and Views across login sessions. If you exit out of a session and log into LMS Portal server later, the LMS Portal page displays the portlets according to your settings.



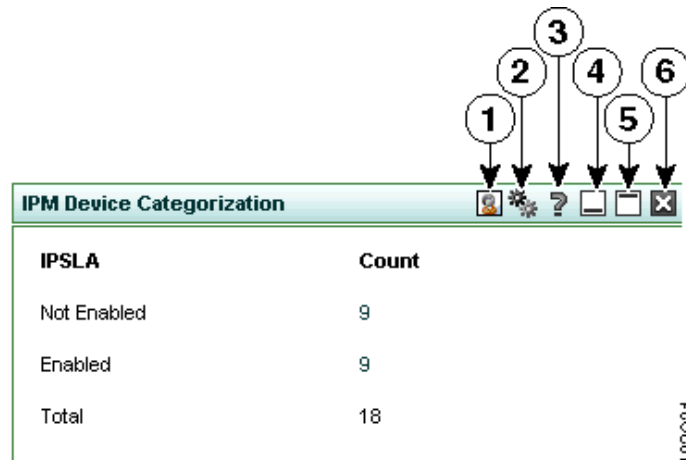
Note

The Network Administrator or a System Administrator configures a list of default portlets in a Public Portal before you can view them.

Each portlet contains six icons on the top right corner and they are visible only when you move the mouse over the portlet name.

See [Figure 5-2](#) to understand the Portlet Icons.

Figure 5-2 Portlet Icons



[Table 5-3](#) lists the Portlet icons as indicated in the figure above.

Table 5-3 Portlet Icons

Number	Icon	Function
1	Look and Feel	Set the look and feel for each portlets. This feature is not available for Functional View portlets.
2	Configuration	Enables you to set the configuration, such as the refresh time, and number of jobs displayed and so on. This feature is not available for Functional View portlets.
3	Help	Opens the context-sensitive help for each portlet.

Table 5-3 Portlet Icons

Number	Icon	Function
4	Minimize	Hides and restores the content of a portlet.
5	Maximize	Enlarges the size of the portlet.
6	Remove	Removes the portlet from the current view. This feature is not available for Functional View portlets.

For further information on portlets and views, see the Online help or *User Guide for LMS Portal 1.1*.

Launching LMS Applications

To launch any CiscoWorks application from the CiscoWorks LMS Portal home page:

-
- Step 1** Launch the CiscoWorks Server in your browser as explained in [Accessing CiscoWorks Server](#).
- Step 2** Click the respective application link or the Home link of the application's portlet in the CiscoWorks LMS Portal home page.

The respective application's home page appears in a new window.

For example, if you select CiscoWorks Assistant from the LMS Portal home page, the CiscoWorks Assistant home page appears with the following TOC items:

- Home
 - Workflows
 - Server Setup
 - Device Troubleshooting
 - End Host/IP Phone Down
 - Administration
 - Log level Settings
-

For more information on this, see the Online help or the *User Guide for CiscoWorks LMS Portal 1.1*.

Launching LMS Workflow Demos

The LMS Workflows Demo portlet displays the most frequently used workflows in LMS 3.1. Click on the workflow to view a demo of it.

The workflows that are listed in the portlet are:

- Using Baseline templates
- Building and exporting a network map using Campus Manager
- Discovering the network
- Using NetConfig to deploy mass configuration changes

- Using SWIM to upgrade device images
- Using User Tracking to find an end host by IP or MAC

**Note**

You must enable JavaScript in the browser window and install the latest version of the Flash Player to view the demo.

Configuring LMS Administration Parameters

After you have installed the required applications and verified the installation, you must perform certain system setup and administrative tasks.

You can perform most of the basic system setup and administrative tasks using the LMS Setup Center.

This section explains the following:

- [Using LMS Setup Center](#)
- [System Setup and Administrative Tasks](#)

Using LMS Setup Center

LMS Setup Center is part of CiscoWorks LAN Management Solution. The LMS Setup Center also allows you to configure the necessary server settings, immediately after installing LMS software.

You can launch the LMS Setup Center, from the CiscoWorks LMS Portal home page. The LMS Setup Center link is enabled only if the LMS license is detected on the system. The following two menu options are available under LMS Setup Center:

- Server Setup

Click on this menu option to launch the CiscoWorks Assistant Server Setup page. You can perform the following Server setup tasks:

- Manage Servers
- Set Default Credentials
- Add Devices
- Allocate Devices
- Change ACS Setup

For more information on this, see the *User Guide for CiscoWorks Assistant 1.1*.

- Server Settings

Click on this menu option to launch the Server settings page. You can do the following server settings:

- System Settings — Configurations that the system needs to function. For example, Backup Schedule and SMTP Server.
- Security Settings — Security related settings for the product. For example, Single Sign On and Authentication Mode.
- Data Collection Settings — Settings to collect data from the devices. For example, SNMP Timeout and Seed Devices.

- Data Collection Schedule — Schedule settings for collecting the data from the server. For example, CM Data Collection Schedule and Inventory Polling Schedule.
- Data Purge Settings — Configurations that are necessary for the device to purge data. For example, Syslog Purge and Number Of Configurations To Keep.

For more information on this, see the LMS Setup Center Online help or the *User Guide for CiscoWorks Common Services 3.2*.

System Setup and Administrative Tasks

The administrative tasks you can perform from each application that you have installed are given below:

Application Name	Administrative Tasks	Launch Point From LMS Portal
Common Services	Manage the CiscoWorks users based on the respective user's access privileges.	You can perform this task using the Local User Setup page. (Common Services > Server > Security > Single-Server Management > Local User Setup).
	Configure the Browser-Server Security. Common Services Server uses Secure Socket Layer (SSL) encryption to provide secure access between the client browser and management server, and also between the management server and devices. You can enable or disable SSL depending on the need to use secure access.	You can perform this task using the Browser-Server Security Mode Setup page. (Common Services > Server > Security > Single-Server Management > Browser-Server Security Mode Setup).
	Configure the SMTP server to receive e-mails from the CiscoWorks server.	You can perform this task using the System Preferences page. (Common Services > Server > Admin > System Preferences). You can also configure this setting during the Server Setup using CiscoWorks Assistant workflow. See About CiscoWorks Assistant for more information.
	Configure the Cisco.com credentials. This information is used while performing some tasks, such as downloading software images, downloading device packages and so on.	You can perform this task using the Cisco.com Connection Management page. (Common Services > Server > Security > Cisco.com Connection Management > Cisco.com User Account Setup).
Common Services (continued)	Configure the proxy URL to access the Internet from the CiscoWorks server, if your system is behind a firewall.	You can do this using the Proxy Server Setup page. (Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup).

Application Name	Administrative Tasks	Launch Point From LMS Portal
Resource Manager Essentials	Assign the protocols to be used in RME for Configuration Management and Software Management.	<ul style="list-style-type: none"> To define the protocol order for fetching and deploying the configuration files, use the Configuration Management page. (Resource Manager Essentials > Administration > Config Management) The available protocols are Telnet, TFTP, RCP, SSH, SCP, and HTTPS. To define the protocol order for Software image import and distribution, use the View/Edit Preferences page. (Resource Manager Essentials > Administration > Software Mgmt > View/Edit Preferences) The supported protocols are: RCP, TFTP, SCP, and HTTP.
	Schedule periodic archive of configuration files (with or without configuration polling).	<p>By default, this is disabled. You can enable this using the Collection Settings page. (Resource Manager Essentials > Administration > Config Management > Archive Management > Collection Settings).</p>
	Change the default schedule of the device inventory collection and polling.	<p>You can do this by using the System Job Schedule page. (Resource Manager Essentials > Administration > Inventory > System Job Schedule).</p>

Application Name	Administrative Tasks	Launch Point From LMS Portal
Campus Manager	<p>Schedule Campus Manager Data Collection.</p> <p>You can schedule the day, time, and frequency of data collection.</p> <p>You can define the periodicity for polling the network.</p> <p>Polling helps you see updated devices and link information without running data collection. Polling is enabled by default.</p> <p>The default poll interval is two hours.</p>	<p>You can perform this task from LMS Portal by selecting Campus Manager > Administration.</p> <p>Click Administration and select Data Collection > Schedule Data Collection in the Schedule Data Collection page.</p>
	Set up Data Collection Filters.	<p>You can specify IP Address ranges for data collection from LMS Portal using the Data Collection Filters page.</p> <p>Select Campus Data Collection > Data Collection Filters.</p>
	<p>Configure User Tracking acquisition actions.</p> <p>User Tracking allows you to locate end-user hosts in the network. It collects and presents information gathered by the Asynchronous Network Interface (ANI) Server and held in the ANI database.</p> <p>You can also use User Tracking to find duplicate connections that could indicate potential problems in your network.</p>	<p>To configure this, from LMS Portal, select Campus Manager > User Tracking and then select Acquisition > Actions in the Actions page.</p>

Application Name	Administrative Tasks	Launch Point From LMS Portal
Device Fault Manager	<p>Adjust polling and threshold settings.</p> <p>The Common Services system-defined groups include groups, such as Broadband Cable, Routers, Switches and Hubs, and so on.</p> <p>These groups have specific polling and threshold settings.</p> <p>The DFM Polling and Threshold function creates its own corresponding groups based on Common Services and DFM groups. These are:</p> <ul style="list-style-type: none"> • Polling groups that determine how often group members are polled for data. • Threshold groups that determine acceptable levels of performance and utilization for group members. 	<p>You can perform this task from LMS Portal using the Polling and Thresholds page.</p> <p>Select Device Fault Manager > Configuration > Polling and Thresholds.</p>
	<p>Set up notifications.</p> <p>In addition to watching network conditions as they change on the Alerts and Activities display, you can use DFM notification services to automatically notify users and other systems when specific changes occur on selected devices.</p> <p>You must create subscriptions for e-mail notifications, DFM-generated SNMP trap notifications, or Syslog notifications.</p>	<p>You can perform this task from LMS Portal using Device Fault Manager > Notification Services in the Notification Services page.</p> <p>You can also change event names to names that are more meaningful to you, and these names will appear in the DFM displays and notifications.</p>
Device Fault Manager (continued)	<p>Add views to the Alerts and Activities Display.</p> <p>The Alerts and Activities display provides a consolidated real-time view of the operational status of your network.</p> <p>When a fault occurs in your network, DFM generates an event (or events). All events occurring on the same device are rolled up into a single alert.</p>	<p>You can perform this task from LMS Portal using the Alerts and Activities Defaults page.</p> <p>(Configuration > Other Configurations > Alerts and Activities Defaults).</p>

Application Name	Administrative Tasks	Launch Point From LMS Portal
Internetwork Performance Monitor	Set the log level.	From LMS Portal, select Internetwork Performance Monitor > Admin > Log Level Settings.
	Automatically update the Common Services' Device Credential Repository (DCR) devices.	From LMS Portal, select Internetwork Performance Monitor > Admin > Application Settings.
	See the IP SLA (Internet Protocol Service Level Agreement) probes for the collectors that you configure.	From LMS Portal, select Internetwork Performance Monitor > Admin > Application Settings.
	Set the purge period for historical data and audit reports.	From LMS Portal, select Internetwork Performance Monitor > Admin > Purge Settings.
Health and Utilization Monitor	Set the log level.	From LMS Portal, select Health and Utilization Monitor > Admin > System Preferences > Log Level Settings.
	Configure HUM to periodically purge job data that you no longer need.	From LMS Portal, select Health and Utilization Monitor > Admin > System Preferences > Job Purge.
	Set Report Publish Location HUM allows you to publish the PDF, HTML and CSV format of all the reports to a directory location of your choice. This is done by setting a default directory path.	From LMS Portal, select Health and Utilization Monitor > Admin > System Preferences > Report Location.
Health and Utilization Monitor (Continued)	Configure HUM to periodically purge polled data that you no longer need in the database. You can purge data records such as Summarization records, Poller failure records, Threshold violation records, Audit Trail records.	From LMS Portal, select Health and Utilization Monitor > Admin > System Preferences > Data Purge
	Configure the frequency of generating Quick Reports	From LMS Portal, select Health and Utilization Monitor > Admin > System Preferences > Quick Report Schedule.
	Configure the SNMP timeout and retries.	From LMS Portal, select Health and Utilization Monitor > Admin > System Preferences > Poll Settings
	Configure the Notification Interval and the E-mail ID for updates about the Polling Failure	From LMS Portal, select Health and Utilization Monitor > Admin > System Preferences > Poll Settings
	Load a new MIB file into HUM using the Load MIB option. The new MIB file is compiled and stored in HUM. You can use the new MIB file to create new templates by grouping MIB variables.	From LMS Portal, select Health and Utilization Monitor > Admin > System Preferences > Load MIB.

For more information on this, see the individual application's User Guide or see the context-sensitive Online help.

Setting Up CiscoWorks Server

You can setup the CiscoWorks Server in a single-server or multi-server environment.

This section explains the following:

- [Before You Begin CiscoWorks Server Setup](#)
- [Setting Up a Single CiscoWorks Server](#)
- [Setting Up Multiple CiscoWorks Servers](#)

Before You Begin CiscoWorks Server Setup

Before you start to set up your CiscoWorks Server, ensure that you understand the following topics:

- [Understanding Single-Server and Multi-Server Setup](#)
- [Understanding DCR and Device Management](#)
- [Understanding Single Sign-On](#)
- [Understanding AAA Modes](#)
- [About CiscoWorks Assistant](#)
- [Methods of Deploying CiscoWorks Server Setups](#)

Understanding Single-Server and Multi-Server Setup

When all the CiscoWorks applications are installed on a single LMS server, the setup is considered as a Single-server setup.

You can also install the CiscoWorks applications in more than one server for better performance and scalability. This setup is considered as a Multi-server setup. The Multi-server setup requires all servers in the setup to work in synchronization with one another.

To setup with multiple CiscoWorks servers, you must:

- Set up Peer Server Account
- Set up System Identity User
- Set Up Peer Server Certificate

You can also enable Single-Sign On so that you can use your browser session to transparently navigate to multiple CiscoWorks Servers without authenticating to each of them. See [Understanding Single Sign-On](#) for more information.

See [Setting Up Multiple CiscoWorks Servers](#) for the information on the terms you need to know and the setup instructions.

Understanding DCR and Device Management

The Device and Credential Repository (DCR) is a common repository of devices, their attributes, and credentials, meant to be used by various network management applications.

DCR helps multiple applications share device lists and credentials using a client-server mechanism, with secured storage and communications. The applications can read or retrieve the information.

These applications can also update the information in DCR so that the updated information could be shared with other applications.

DCR also allows you to populate the repository by importing devices from many sources. It also allows you to export device data to be used with third-party network management systems such as NetView and HP OpenView Network Node Manager.

To understand DCR, see the following topics:

- [DCR Modes](#)
- [Device Management Modes](#)

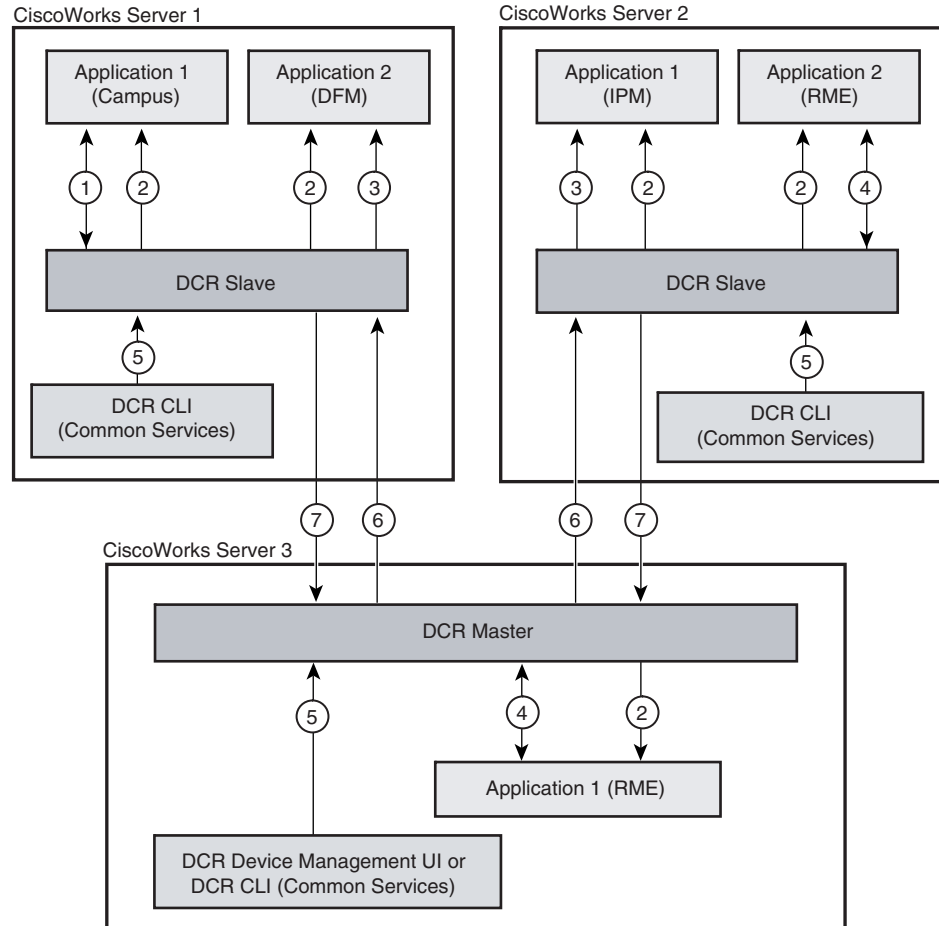
See *User Guide for CiscoWorks Common Services 3.2* for more information.

DCR Modes

The sharing of device list and credentials among various network management products is achieved through a Client-Server mechanism. The clients are network management applications that use DCR. The server is called the DCR Server.

DCR works based on a Master-Slave model. DCR Server can also be in Standalone mode.

[Figure 5-3](#) explains the DCR Master-Slave interactions.

Figure 5-3 DCR Master-Slave Interaction

1. Applications such as Campus Manager add, fetch, and update devices and credentials
2. DCR Server notify changes to the applications
3. Applications such as IPM and DFM fetch devices and credentials from DCR
4. Applications such as RME fetch and update devices and credentials
5. DCR CLI and Device Management UI add/delete devices, update device credentials, and import/export devices
6. DCR Master notifies DCR Slaves for add, update, and delete devices and credentials
7. DCR Master pulls updated devices and credentials from DCR Slave in response to its notification

183883

Master DCR

The master repository of device list and credential data. 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 Slave mode, normally shares this list.

There is only one Master repository for each management domain, and it contains the most up-to-date device list and credentials.

Slave DCR

The Slave DCR is a repository that is an exact replica of the Master.

DCR Slaves are slave instances of DCR in other servers and provide transparent access to applications installed in those servers.

Any change to the repository data occurs first in the Master, and those changes are propagated to multiple Slaves. There can be more than one Slave in a management domain.

The Slave:

- Maintains an exact replica of the data managed by the Master for the management domain.
- Has a mechanism to keep itself synchronized with the Master.
- Will first update Master and then update its own repository data. This is in case of repository data updates.



Note

If the AAA mode is set to ACS, ensure that all the servers within the DCR Master-Slave domain are in ACS mode.

Standalone DCR

In Standalone mode, DCR maintains an independent repository of device list and credential data. It does not participate in a management domain and its data is not shared with any other DCR. It does not communicate with or contain registration information about any other Master, Slave, or Standalone DCR.

The DCR mode is set to Standalone, by default, after a fresh installation of Common Services on the CiscoWorks Server.

DCR running in Master or Slave mode always has an associated DCR Group ID that indicates the Server's management domain. This Group ID is generated when a DCR is set to Master mode, and communicated to all Slaves that are later assigned to that Master.

In Single-Server Setup, the DCR mode is set to Standalone by default.

Device Management Modes

The Device Management mode determines whether the new devices are automatically managed by CiscoWorks applications.

The possible modes are:

- Auto Allocation Off

In this mode, automatic addition of devices to LMS applications is disabled. You can use this option to:

- Selectively add devices to the application from DCR.
- Add the previously deleted devices back into the application.

You can manually add the devices to LMS applications even if you have selected other modes for device management.

- Auto Allocation—All Devices

In this mode, all the devices in DCR are added to the selected LMS application. This is also limited by the LMS license you have purchased.

For example, if you bought a license that allows you to manage 300 devices, you will be able to add and manage only 330 devices (license limit + 10%) in the applications.

- Auto Allocation—Allocate by Groups

In this mode, devices that belong to a specific group in Common Services are added to LMS applications. This is also limited by the LMS license you have purchased. You must select the group name for all applications installed in local and peer servers.

New devices added into the group after applying the settings, will be dynamically added into applications.

**Note**

You can change the Device Management mode of LMS applications by either using the respective applications or by using CiscoWorks Assistant Server Setup workflow.

Table 5-4 helps you understand the Device Management modes for the respective applications.

Table 5-4 Device Management Modes

Application	Default Device Management Mode in Application	Description
Campus Manager	Auto Management—All Devices	<p>The devices in DCR are automatically managed in Campus Manager Data Collection.</p> <p>In Auto mode you can either manage all devices or manage devices in groups. To do so, select Campus Manager > Administration > Data Collection > Device Management > Mode And Policy Settings.</p> <p>You can also add manually the devices to Campus by selecting Campus Manager > Admin > Data Collection > Device Management > Include Devices.</p> <p>For more details on this, see the Administering Campus Manager chapter of the <i>User Guide for Campus Manager 5.1</i>.</p>
Device Fault Manager	Auto Allocation Off	<p>You must manually add the devices from DCR into DFM inventory.</p> <p>To import the devices, select Device Management > Device Import from the DFM home page.</p> <p>From the device import page, you can also:</p> <ul style="list-style-type: none"> • Automatically import all devices from DCR. • Automatically import only the devices which you want to import from DCR using the device group filters. <p>For more information, see the <i>User Guide for Device Fault Manager 3.1</i>.</p>

Application	Default Device Management Mode in Application	Description
Internetwork Performance Monitor	Auto Allocation Off	<p>To Manually import DCR devices, go to Internetwork Performance Monitor > Collector Management > Devices > Add Devices.</p> <p>You can use the Auto Allocation Settings option to enable automatic allocation of devices to IPM from Device Credentials Repository (DCR).</p> <p>To change the device management settings, go to LMS Portal and select Internetwork Performance Monitor > Admin > Auto Allocation Settings.</p> <p>For more detailed information on this, see the <i>User Guide for Internetwork Performance Monitor 4.1</i>.</p>
Resource Manager Essentials	Auto Management—All Devices	<p>Whenever you add devices to Device and Credential Repository, RME triggers the Device Auto Management service.</p> <p>The devices that are added to Device and Credential Repository get automatically added to RME.</p> <ul style="list-style-type: none"> You can enable the Device Auto Management setting from Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings. You can add devices to RME manually from Resource Manager Essentials > Devices > Device Management > RME Devices > Add Devices. You can add devices to RME using the <code>cwcli inventory</code> command. See RME Device Management Using cwcli Inventory Command for more information. <p>For more detailed information on this, see the Online Help or see the <i>User Guide for Resource Manager Essentials 4.2</i>.</p>

Understanding Single Sign-On

The Single Sign-On (SSO) feature helps you to use a single session to navigate to multiple CiscoWorks servers without having to authenticate to each of them.

SSO mode can be set as Standalone, Master or Slave. In a single-server setup, the SSO mode is usually set to Standalone.

The following tasks need to be done initially to enable SSO:

- One of the CiscoWorks Servers should be set up as the authentication server. The SSO authentication server is called the Master, and the SSO regular server is called the Slave. If there is no SSO Master server configured in your setup, the local server is selected as SSO Master.
- Trust should be built between the CiscoWorks Servers, using self signed certificate. You should configure Master's Self Signed Certificate in Slaves.
- Each CiscoWorks Server should setup a shared secret with the authentication server. The System Identity user password acts as a secret key for SSO.

See the Enabling Single Sign-On section in *User Guide for CiscoWorks Common Services 3.2* for more information.

Understanding AAA Modes

CiscoWorks Server has some built-in security features to authenticate and authorize users to perform the tasks in CiscoWorks applications. CiscoWorks Server also provides a way to select and configure pluggable authentication sources.

To get maximum security protection, CiscoWorks Server can be integrated with Access Control Server (ACS). When integrated all the authentication and authorization transactions are performed by that ACS server.

The following are the AAA modes in CiscoWorks Server:

- Non-ACS — Also called CiscoWorks local mode. All the authentication services are provided by the login modules selected.

The available login modules are:

- CiscoWorks Local
 - IBM SecureWay Directory
 - KerberosLogin
 - Local UNIX System
 - Local NT System
 - MS Active Directory
 - Netscape Directory
 - Radius
 - TACACS+
- ACS — See [Integrating CiscoWorks Server with ACS](#) for more information.

About CiscoWorks Assistant

CiscoWorks Assistant is a web-based tool that provides workflows to help you to overcome network management and software deployment challenges.

CiscoWorks Assistant provides workflows which contain functionalities that are available across LMS applications. These functionalities are grouped logically to setup and configure the LMS server and to troubleshoot your network devices.

CiscoWorks Assistant supports the following workflows:

- **Server Setup**

Server Setup workflow helps you to create a single or multi-server setup. It also assists you to add and manage devices, as well as configure the AAA mode to ACS.

You can add devices to Device and Credential Repository by performing bulk import from file or NMS, or by using the Common Services Device Discovery.

You can set the Device Management mode to determine whether the new devices added, are automatically managed by CiscoWorks applications.

- **Device Troubleshooting**

You can identify the root cause for device unreachability. The generated Device Troubleshooting report contains the following details:

- Device reachability
- Alerts and Syslog messages
- Differences between the two archived running configurations.
- Changes in the device configuration file, inventory, and installed image
- Details of the device topology
- Check Device Attributes (CDA) information
- Details on network inconsistencies, misconfiguration in the physical and logical layout in the discovered network.

- **End Host/IP Phone Down**

You can get the information required to troubleshoot as well as analyze the connectivity issues.

Methods of Deploying CiscoWorks Server Setups

You can either deploy a single-server or multi-server setups:

- **Using Common Services and other LMS applications**

This is a traditional method of deploying single-server setup or multi-server setup in your network. You should manually configure each and every server setup tasks.

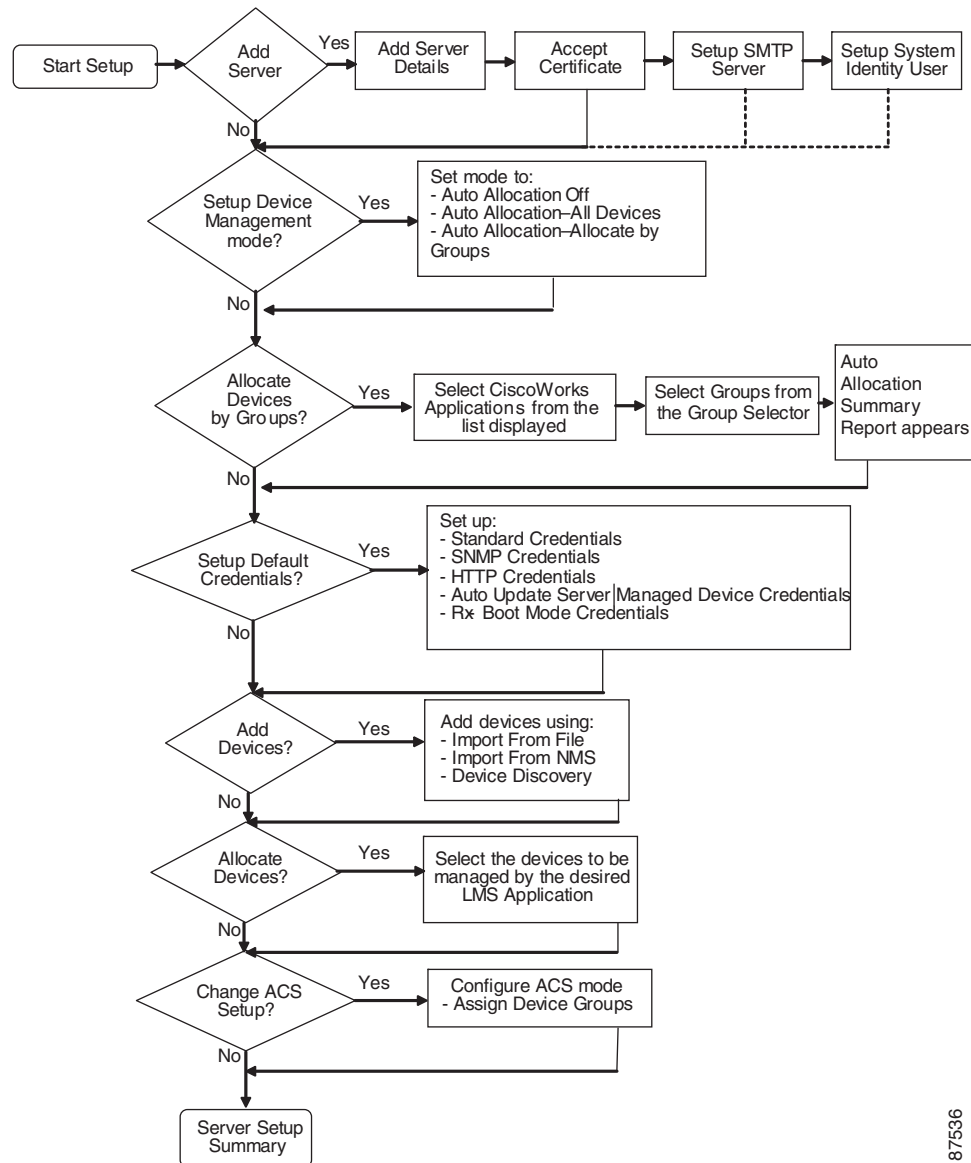
Or

- **Using CiscoWorks Assistant Server Setup workflows**

The Server Setup workflow in CiscoWorks Assistant helps you to setup and manage CiscoWorks LAN management Solution (LMS) servers. It helps you to simplify the deployment and setting up of single or multiple LMS servers using the wizard based dialog boxes.

With this workflow, you need not go to each application to perform the server setup tasks.

[Figure 5-4](#) helps you to understand the workflow.

Figure 5-4 Workflow to Deploy a Single CiscoWorks Server

187536

See *User Guide for CiscoWorks Assistant 1.1* for instructions on how to navigate within a Server Setup workflow.

This document explains how to set up the CiscoWorks Server using the CiscoWorks Assistant Server Setup workflow.

See [Setting Up a Single CiscoWorks Server](#) and [Setting Up Multiple CiscoWorks Servers](#) for more information.

Setting Up a Single CiscoWorks Server

To deploy a single CiscoWorks Server in your network, you should perform the following tasks using CiscoWorks Assistant Server Setup workflows:

- [Manage LMS Server](#)
- [Set up Device Management Mode](#)
- [Set up Default Credentials](#)
- [Add Devices](#)
- [Manage Devices in the Applications Installed in the LMS Servers](#)

Additionally, you can change the login module of CiscoWorks Server to ACS using the Server Setup workflow. See [Integrating CiscoWorks Server with ACS](#) for more information.

Manage LMS Server

The Manage Servers page displays the details of the local CiscoWorks Server that you have configured during CiscoWorks Installation or after the installation using the other CiscoWorks applications such as Common Services and LMS Setup Center.

To modify the server details:

Step 1 Select **CiscoWorks Assistant > Workflows > Server Setup > Manage Servers**.

Step 2 Select the server by clicking the Host Name/IP Address radio button, and click **Edit**.

The Edit Server dialog box appears.

This dialog box has pre-populated values in Hostname/IP address, Protocol, Port and Current SSO Settings fields. All fields in the Edit Server dialog box can be edited, except the Hostname/IP address, Protocol, Port, and Current SSO settings fields.

- If the server is in SSO Slave mode, you can set it as SSO Master, by selecting the Set as Master check box.
- If the server is in SSO Master Mode, you can change it to Slave mode by selecting the Set as Slave check box. The Set as Slave check box is not present in the local server.

Step 3 Enter the Server Details and Setup parameters in the Edit Server dialog box, and click **OK**.

Step 4 Click **Next**.

The Current System Identity User pop-up appears.

In a Single-server setup, if you have provided the admin user name and password, you will not be prompted to enter System Identity User details.

Step 5 Click **OK** after you enter the System Identity User details.

The New System Identity User window appears.

You can either:

- Enter the new System Identity Username and Password, Confirm Password, and click **Next**

Or

- Click **Skip** to proceed, if you do not want to change the current System Identity User.

**Note**

The System Identity Setup is required when you want to integrate the CiscoWorks Sever with ACS Server or when you want to setup the multi-server. Otherwise, you can skip this step.

The Device Management Mode page appears.

Step 6 Click **Next**, after you modify the Device Management mode.

If you do not want to change the settings, click **Next** when you get to this page without making any modifications to the existing Device Management mode. The Skip button is disabled in this page.

The workflow initiates after you click **Next**. The modifications you made are saved when the tasks are complete.

Set up Device Management Mode

The Device Management mode determines whether the new devices are automatically managed by CiscoWorks applications. By default, the mode is set to Auto Management mode for all installed applications except DFM and IPM. The default mode of DFM and IPM is manual allocation of devices.

However, you can change the Device Management mode when needed.

To set the Device Management mode:

Step 1 Click **Next**, after adding the server or setting up the System Identity User.

The Device Management Mode page appears.

The possible modes are:

- Auto Allocation Off
- Auto Allocation—All Devices
- Auto Allocation—Allocate by Groups

For details on the above modes, see [Device Management Modes](#).

By default, the Device Management mode shows the current status of device management mode of applications that have been set up in their respective Device Management Settings pages.

Step 2 Select any one of the following from the drop down list for each CiscoWorks server application:

- Auto Allocation Off
- Auto Allocation—All Devices
- Auto Allocation—Allocate by Groups

Step 3 Click **Next**.

The workflow performs the assigned tasks when you click **Next** in the Device Management Mode page.

The Manage Servers Progress page appears with the Server Management Status.

The process of checking the status of various tasks might take some time.

You can either:

- Set up CiscoWorks Assistant to send you an e-mail notification. You can then exit from the workflow before the tasks are complete. You can come back to view the status after you get the e-mail notification that the tasks have completed.

See Setting up E-mail Notification After Managing Server Tasks in the *User Guide for CiscoWorks Assistant 1.1* for details.

Or

- Wait until the status check has completed to view the status.

The status on the following tasks are displayed:

- Configuring SMTP Server and e-mail.
- Device Management mode configuration.

Step 4 Click on the relevant step link to view the detailed status report for that step.

If a step fails, the **Last Accessed URL** column in the report will display the shortcut URL for that particular step. The column will be blank, if the step is successful.

Set up Default Credentials

Devices added or imported into DCR do not contain all credentials required by the network management applications to manage them. Sometimes this could lead to the failure of application jobs.

The default credentials feature helps you to add or import devices into DCR with the default credentials and prevents the management applications from failing when the network management applications manage the devices added or imported in DCR.

Default credentials are stored in DCR and are not associated with any device. DCR maintains only one default credential set comprising the following credentials:

- Primary Credentials (Username, Password, Enable Password)
- Secondary Credentials (Username, Password, Enable Password)
- SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)
- SNMPv3 Credentials (Username, Password, Authentication Algorithm, Privacy Password, Privacy Algorithm)
- HTTP Credentials (Primary HTTP Username and Password, Secondary HTTP Username and Password, HTTP port, HTTPS port, Current Mode)
- Auto Update Server Managed Device Credentials (Username and Password)
- RxBoot Mode Credentials (Username, Password)

To set the default device credentials, select **CiscoWorks Assistant > Workflows > Server Setup > Set Default Credentials**. The Default Credentials page appears.

The following are the set of default credentials that you are required to set in order to complete the server setup:

- Set Standard credentials
- Set SNMP credentials
- Set HTTP credentials
- Set Auto Update Server managed Device credentials
- Set RxBoot Mode credentials

You can subsequently configure the ACS mode and assign device groups.

For more details, see the Setting Default Credentials section in the *User Guide for CiscoWorks Assistant 1.1*

Add Devices

You can use this feature to add devices, device properties or attributes, and device credentials to the DCR.

You should have the required privileges to add devices to DCR. Your login determines whether you can use this option.

Methods of Adding Devices

You can add devices to the Device and Credentials Repository (DCR) using the following methods in CiscoWorks Assistant:

- Bulk Import from File
You can import device lists, device properties or attributes, and device credentials to the DCR using CSV or XML files.
- Bulk Import from Network Management Station (NMS)
You can import device lists and device credentials from the local or remote Network Management Systems.
- Device Discovery

Device Discovery allows to discover the devices from the network starting from the seed devices. It updates the device information in DCR. Device Discovery data contains the information about the neighboring devices of seed devices that you have specified.

Note the following about Device Discovery:

- You should have the Network Administrator privileges to configure Device Discovery settings and start Device Discovery.

However to view the Device Discovery summary, you should have any one of the following roles assigned to you:

- Network Administrator
- Network Operator
- System Administrator
- You can only discover Standard devices and Cluster Managed devices through the Device Discovery feature. You cannot discover AUS Managed and CNS Managed devices from the network.

- When DCR or DCR Administration is down, you cannot start Device Discovery. However, you can configure Device Discovery settings.

Scheduled jobs that were started before DCR Administration went down, complete successfully. However, DCR is not updated with the new device credentials returned from Discovery.

- You can run Device Discovery in ACS mode and in a Master-Slave setup.

Device Discovery populates the Device and Credentials Repository with the following discovered information:

- Host name, System name, sysObjectID, IP Address of the neighboring devices, Status of the device, and the module used to discover the device.

You can configure Device Discovery from **Common Services > Device and Credentials > Device Discovery > Discovery Settings**.

For complete details on this, see *User Guide for Common Services 3.2*.

CiscoWorks Assistant allows you to add devices using multiple methods simultaneously. You can add devices using the Import from File feature, and Device Discovery at the same time.

Adding Devices Using Server Setup Workflow

You can use this feature to add devices, device properties or attributes, and device credentials to the Device and Credential Admin.

You should have the required privileges to add devices to DCR. Your login determines whether you can use this option.

Methods of Adding Devices

You can add devices to the Device and Credentials Repository (DCR) using the following methods in CiscoWorks Assistant:

- Bulk Import from File

You can import device lists, device properties or attributes, and device credentials to the DCR using CSV or XML files.

- Bulk Import from Network Management Station (NMS)

You can import device lists and device credentials from the local or remote Network Management Systems.

- Device Discovery

Device Discovery allows you to discover the devices from the network starting from the seed devices. It updates the device information in DCR. Device Discovery data contains the information about the neighboring devices of seed devices that you have specified.

Adding Devices Using Server Setup Workflow

To add devices using the Server Setup Workflow in CiscoWorks Assistant:

Step 1 Go to **CiscoWorks Assistant > Workflows > Server Setup > Add Devices**.

The Add Devices page appears.

Step 2 Select one or more of the following methods to add devices:

- [Import From File](#)
- [Import From NMS](#) (either Local NMS or Remote NMS)
- [Run Discovery](#) (Common Services Device Discovery)

If you select **Import From File**:

- a. Enter the file name or use the browse button to select the file to import the devices.
- b. Select a file format. You should select either CSV or XML.
- c. Select either **Use data from Import source** or **Use data from Device and Credential Repository**, to resolve conflicts that may occur if the devices are present both in the import source and DCR, but differ in their attributes.
 - If you select **Use data from Import source**, the credentials from the import source will be used, and credentials for the device in DCR will be modified.
 - If you select **Use data from Device and Credential Repository**, the device credentials in DCR will be used.
- d. Select the Use Default Credentials check box to use the default credentials to import the devices. See [Set up Default Credentials](#) to know about the default credentials.

If you select **Import From NMS** and want to import the devices from Local NMS:

- a. Select the Network Management System type from the NMS type drop-down list. For the supported versions, see [Supported Network Management Systems](#).
- b. Enter the installation location of Network Management System in the Install Location field.
For example: C:\Program Files\HP OpenView
- c. Select either **Use data from Import source** or **Use data from Device and Credential Repository**, to resolve conflicts that may occur if the devices are present both in the import source and DCR, but differ in their attributes.
 - If you select **Use data from Import source**, the credentials from the import source will be used, and credentials for the device in DCR will be modified.
 - If you select **Use data from Device and Credential Repository**, the device credentials in DCR will be used.
- d. Select the Use Default Credentials check box to use the default credentials to import the devices. See [Set up Default Credentials](#) to know about the default credentials.

If you select **Import From NMS** and want to import the devices from Remote NMS:

- a. Select the Remote NMS check box.
- b. Select the Network Management System type from the NMS type drop-down list. For the supported versions, see [Supported Network Management Systems](#).
- c. Select the Operating System type from the OS type drop-down list.
- d. Enter the host name, root username, and install location in the corresponding fields.
If you select the NMS type as ACS, enter the root password, port and protocol along with the hostname and root username in the corresponding fields.
- e. Select either **Use data from Import source** or **Use data from Device and Credential Repository**, to resolve conflicts that may occur if the devices are present both in the import source and DCR, but differ in their attributes.
- f. If you select **Use data from Import source**, the credentials from the import source will be used, and credentials for the device in DCR will be modified.
- g. If you select **Use data from Device and Credential Repository**, the device credentials in DCR will be used.
- h. Select the Use Default Credentials check box to use the default credentials to import the devices. See [Set up Default Credentials](#) to know about the default credentials.

If you select **Run Discovery**:

a. You need to select any one of the following Discovery modules :

- Address Resolution Protocol
- Border Gateway Protocol
- Open Shortest Path First Protocol
- Routing Table
- Cisco Discovery Protocol
- Ping Sweep On IP Range
- Cluster Discovery
- Hot Stand by Router Protocol

b. You need to give the following inputs for the Seed Devices Tab:

- IP Address or hostname of the seed device
- Number of hops in the Hop Count field

For Cisco Discovery Protocol, you can select the Jump Router Boundaries option, to extend Discovery beyond the boundaries set by routers on your network.

You must be cautious about enabling Discovery to occur beyond router boundaries. Discovery could take much longer if you do not selectively choose the boundaries by excluding specific IP addresses.

Enter the following fields that appear only for Ping Sweep On IP Range Discovery module.

- ICMP Retry— No of retries to connect to a device using ICMP protocol if the device is not reachable or network is down. The default is 1 retry.
- ICMP Timeout— Time within which the device should send its response to the network. The default timeout is 1000 milliseconds.
- InterPacket Timeout—Time delay between two ICMP packets. The default timeout is 20 milliseconds.

c. In the SNMP Tab:

You can configure SNMP credentials to run Device Discovery. You must configure either SNMPv2 or SNMPv3 credentials.

For SNMP v2, enter the following details:

- SNMP Version—Version of the SNMP protocol
- Target—Target device.
- Read Community—Read community string.
- Time Outs—Time period after which the query times out.
- Retries—Number of attempts.
- Comments—Remarks, if any.

For SNMP v3, enter the following details:

- Target—Target device.
- User Name—Name of the user who has access to views configured on the device.
- Auth Password—SNMP V3 authentication password used to operate the devices in AuthNoPriv and AuthPriv modes.

- Auth Algorithm—SNMP V3 authentication algorithm used in AuthNoPriv and AuthPriv modes. The authentication algorithm can be MD5 or SHA-1.
- Privacy Password—SNMP V3 privacy password of the device in AuthPriv mode.
- Privacy Algorithm—SNMP V3 privacy algorithm used in AuthPriv mode. The privacy algorithm can be DES, 3DES, AES128, AES192, and AES256.
- Time Outs—Time period after which the query times out.
- Retries—Number of attempts.
- Comments—Remarks, if any.

d. Filter Settings tab

Filters allow you to include or exclude devices from the network.

You can select a filter from the Use Filter drop-down list. The supported filters are:

- IP Address
- DNS Domain
- SysObjectID

For SysObjectID filter, you can either enter the value manually or select a SysObjectID from the Device Type Selector. The Device Type Selector appears after you have selected a SysObjectID filter from the Use Filter drop-down list.

- SysLocation

You can either include or exclude a filter by selecting either the Include or Exclude radio buttons. From the filter settings you can add and delete a filter.

e. Global Settings Tab:

- Preferred DCR Display Name— This can be any of these:
 - IP Address—Preferred management IP Address of the device.
 - Hostname—DNS resolvable name of preferred management IP Address.
 - FQDN — Fully Qualified Domain Name. This consists of a hostname and a domain name.
- Preferred Management IP Address—This can be any of these:
 - Use LoopBack Address—Resolves the server name by loopback address. If the device has an IP address for LoopBack Interface, the device is managed using this IP address.
 - If there are multiple Loopback IP addresses, one of them is used to manage the device.
 - Resolve By Name—Select this option if you have configured the device with DNS Name. This name is fetched from DNS during Discovery.
 - Resolve By Sysname—Contacts the DNS server to get the device hostname.
 - None —Select this option if you do not want to manage the devices with the preferred management IP Address. If you select this option, the devices are added in DCR with their IP Addresses.
 - The Resolve By Name option is the default option for this field.
- Add Discovered Devices to a Group— Select this checkbox to add the discovered devices to a group.

- Group Name—Displays the name of the group you have selected already. You can also change the group name.

Click **Select**. The Select a Group popup window opens. You can specify a new group name or select an existing group. The Select button is enabled only when the Add Discovered Devices to a Group option is enabled.

- Use Default Credentials—When you select this option, devices that are discovered and updated to DCR will be associated with the default credentials.
- Update DCR Display Name—Select this option to update the Display Name of Device in DCR.
- E-mail— Enter a valid e-mail ID in this field. Multiple e-mail IDs are not allowed in this field. The system uses the e-mail ID to notify you about the status of the Device Discovery jobs.

Step 3 Click **Next** to go to Manage Devices wizard.

Manage Devices in the Applications Installed in the LMS Servers

You can select devices from the device selector and add it to the application with which you want the device to be managed.

You can also:

- View Device Management status
- Use Device Selector to search for devices in DCR

To manage devices:

Step 1 Select **CiscoWorks Assistant > Workflows > Server Setup > Allocate Devices**.

The Manage Devices page appears.

Step 2 Go to the Device Selector and select the devices that you want to add.

Step 3 Select the applications to which you want to allocate the devices.

Initially, devices must be added to DCR. After a device is added to DCR, you can add it to the applications.

Step 4 Click **Add Devices** to add devices.

Or

Click **Reset** to reset the added devices in the application.

The Manage Devices screen displays:

- LMS Server—LMS Server IP Address
- Applications—Applications installed in the LMS Server
- Selected Devices—Number of devices selected to add in that application

Step 5 Click **Next** to complete the Manage Devices tasks.

The Device Management Progress page appears. You can view the Device Management status in this page.

The Server Setup Summary page appears with a summary of Session details, Server Summary and the Operational details. For more details, see the Viewing Server Addition Summary section in the *User Guide of CiscoWorks Assistant 1.1*.

After adding devices, you can:

- [View Device Allocation Summary](#)
- [Search for Supported Devices](#)

View Device Allocation Summary

In the Device Allocation Summary portlet, you can view the summary of all the devices managed by each application. The portlet also displays the details of the devices that are not managed by the corresponding application.

In a Master- Slave setup when the same device is managed by both Master and Slave in an application, it creates a duplicate entry. However, the Device Allocation Summary portlet displays the count after deleting the duplicate entry.

[Table 5-5](#) lists the Device Allocation Summary portlet details.

Table 5-5 **Details of Device Allocation Summary**

Field	Description
Application	Displays the name of the applications managing devices such as Resource Manager Essentials (RME), Device Fault Manager (DFM), Health and Utilization Monitor (HUM), Campus Manager (CM) and Internetwork Performance Monitor (IPM).
Managed Devices	Displays the number of devices managed by the corresponding application. You can click Device Count to launch the devices managed by the Application report. The report displays the server name and the managed device count.
Total no.of devices in the server	Displays the total number of devices in the server.
Devices not managed by any application.	<ul style="list-style-type: none"> • In Non-ACS mode: Displays the total number of devices not managed by any of the application. • In ACS mode: Displays the total number of devices neither configured in ACS nor managed by any of the application.

Search for Supported Devices

The Supported Device Finder portlet enables you to view the details of the devices that are supported in various LMS applications such as Resource Manager Essentials (RME), Campus Manager (CM), Device Fault Manager (DFM), and CiscoView.

By default the Supported Device Finder portlet is added in the System View.

This portlet enables you to:

- Locate the supported devices in the LMS applications
- Get the latest updates on devices that are supported and those that will be supported in the upcoming releases.
- Raise a request through email to support a new device if it is not supported.

You can search the support of devices added to the DCR using the following search options:

- IP Address
- Host Name
- Display Name
- Model Name
- SysObjectID

To search using Supported Device Finder portlet:

Step 1 Select an option from the drop-down list and enter the corresponding value in the field and click **Submit**.

For example, if you have selected SysObjectID as the option, enter the SysObjectID in the field.

- If the device is supported, the following details appear in the portlet:
 - SysObjectID
 - Model Name
 - Application Name along with Support details and Comments.
- If the device is not supported in the current installation the following message appears:

The device is not supported. Click here for more information.
- If the requested device is supported in later releases, and not available with your present installation, the following message appears:

Not supported in Installed version <<version number>>.Support available in version <<version number>>



Note If the device is currently not supported with your existing package, you can install the latest IDU from Cisco.com to get device support.

- If the requested device is not supported in any releases, the following message appears:

The device is not supported. Click here for more information.

Step 2 Click the Click Here link.

A pop-up box appears with the following information:

- OK button—To raise a request for the unsupported device.
- Disclaimer : Please note that all efforts will be made to provide support to this request. However, we cannot commit to a time-period at present.

- Links to the latest device updates on Campus Manager, Device Fault Manager and CiscoView
- Link to the Supported Devices Table

Step 3 Click **OK** to raise a request for *SysobjectID* or *Model name*

The SysobjectID or the Model Name appears based on the entries made in the portlet.

The default mail client is launched.

The To field and Subject field have the following address and entries:

- To field: lms-dev-supreq@external.cisco.com
- Subject field: Request for new Device Support *SysobjectID* or *Model name*
- Body: Lists the application names.

Step 4 Enter **Yes** against the respective application names for which device support is required.

Step 5 Click **Send** to send a request.

Setting Up Multiple CiscoWorks Servers

You can set up a multi-server environment by performing the following:

- [Terms and Definitions](#)
- [Before Setting Up Multi-Servers](#)
- [Multi-Server Setup Tasks](#)

Terms and Definitions

Before you set up a multi-server environment you should know the following terms and definitions:

- [Peer Server Account Setup](#)
- [System Identity Setup](#)
- [Peer Server Certificate Setup](#)

Peer Server Account Setup

Peer Server Account Setup helps you create users who can programmatically login to CiscoWorks servers and perform certain tasks. These users should be set up to enable communication among multiple CiscoWorks servers. You can set up the Peer Server account in Common Services.

See the Setting Up Peer Server Account section in *User Guide for CiscoWorks Common Services 3.2* for more information.

System Identity Setup

Communication among multiple CiscoWorks servers is enabled by a trust model addressed by certificates and shared secrets. System Identity setup should be used to create a trust user on peer servers to facilitate communication in Multi-server scenarios. This trust user is called System Identity User.

A default System Identity User admin is created during installation. While installing, you must enter the password for System Identity user. This password can be different from the password you provide for the admin user to log in to CiscoWorks.

You can also create the System Identity User using Common Services or using the Server Setup workflow of CiscoWorks Assistant.

Peer Server Certificate Setup

Peer Server Certificates are used to allow one CiscoWorks server to communicate with another, using SSL. In a multi-server setup, you have two or more servers on which CiscoWorks applications are installed. CiscoWorks allows you to add the certificate of another CiscoWorks server (a peer server) into its trusted store.

Before Setting Up Multi-Servers

Before you begin to setup Multi Servers, you need to:

- [Decide on the DCR Master Server](#)
- [Decide on the SSO Master Server](#)
- [Import Peer Server Certificates in all the Servers in the Setup](#)

Decide on the DCR Master Server

In a Multi-Server setup, Server Setup workflow runs only on the DCR Master server.

You can set up the DCR mode of the server which you want work as a Master and run the Server Setup workflow in that Master server.

In Server Setup workflow, the local server will be treated as DCR Master server if the setup is converted from Single-Server setup to Multi-Server setup. In other words, the DCR mode of the local server will be changed from Standalone to Master, if you add a new server to the local server.

Decide on the SSO Master Server

A Multi-Server setup must have one SSO Master. The other LMS servers must be in SSO Slave mode. If there is no SSO Master server configured in your setup, the local server is set as SSO Master.

You can configure any other server in the setup as a SSO Master. It is not mandatory that the local server serving as DCR Master be configured as SSO Master.

If the SSO Master is not reachable, you cannot perform any operation in the Server Setup workflow. Also, if any of the servers is unreachable, you cannot perform the Manage Servers and Change ACS Mode Setup steps.

Import Peer Server Certificates in all the Servers in the Setup

You should import the peer server certificate details in all other servers in the same domain. See [Peer Server Certificate Setup](#) for more information.

Multi-Server Setup Tasks

To deploy multiple CiscoWorks Server in your network, you should perform the following tasks using CiscoWorks Assistant Server Setup workflows:

- [Manage CiscoWorks Servers](#)
- [Set up Device Management Mode For Applications in All Servers](#)
- [Set up Default Credentials in DCR Master](#)
- [Add Devices to DCR](#)
- [Manage Devices in the Applications Installed in All DCR Servers](#)

**Note**

The Server Setup workflows runs only on DCR Master server.

Additionally, you can change the login module of CiscoWorks Server to ACS using the Server Setup workflow. See [Integrating CiscoWorks Server with ACS](#) for more information.

Manage CiscoWorks Servers

The Manage Servers page displays the CiscoWorks Server Details. This page allows you to:

- Edit local server details
- Add server details
- View server details
- Set up System Identity User
- Set up the Device Management mode
- Delete server

For more information on this, see the Online Help or the *User Guide for CiscoWorks Assistant 1.1*.

This section explains the following:

- [Editing Local Server](#)
- [Adding Server Details](#)

Editing Local Server

To edit a server:

Step 1 Select **CiscoWorks Assistant > Workflows > Server Setup > Manage Servers**.

Step 2 Select the server by clicking the Host Name/IP Address radio button, and click **Edit**.

The Edit Server dialog box appears.

This dialog box has pre-populated values in Hostname/IP address, Protocol, Port and Current SSO Settings fields. All fields in the Edit Server dialog box can be edited, except the Hostname/IP address, Protocol, Port, and Current SSO settings fields.

- If the server is in SSO Slave mode, you can set it as SSO Master, by selecting the Set as Master check box.
- If the server is in SSO Master Mode, you can change it to Slave mode by selecting the Set as Slave check box. The Set as Slave check box is not present in the local server.

- Step 3** Enter the Server Details and Setup parameters in Edit Server dialog box, and click **OK**.
- Step 4** Click **Next**.
The Current System Identity User pop-up appears.
- Step 5** Enter the System Identity User details.
In a Multi-server setup, if you have provided admin user name and password for all servers, you will not be prompted to enter System Identity User details.
- Step 6** Click **OK**.
The New System Identity User window appears.
- Step 7** Either:
- Enter the new System Identity Username and Password, Confirm Password, and click **Next**.
- Or
- Click **Skip** if you do not want to change the current System Identity User.
- The Device Management Mode page appears.
- Step 8** Click **Next**, after you modify the Device Management Mode.
If you do not want to change the settings, click **Next** when you get to this page without making any modifications to the existing Device Management mode. The Skip button is disabled in this page.
The workflow initiates after you click **Next**. The modifications you made are saved when the tasks are complete.
-

For more information on this, see the Online Help or the *User Guide for CiscoWorks Assistant 1.1*.

Adding Server Details

To add a CiscoWorks server:

-
- Step 1** Select **CiscoWorks Assistant > Workflows > Server Setup > Manage Servers**.
- Step 2** Click **Add**.
The Add Server dialog box appears.
- Step 3** Enter the following server details:
- Hostname/IP Address—Hostname or IP Address of the CiscoWorks server. If the server you add is in DCR Master mode, or if it is the Slave of another DCR master, it will not allow you to add the server.
 - Administrator Username—Admin username for the server.
 - Administrator Password—Admin password for the server.
 - Protocol—Protocol of the server. Select HTTP or HTTPS from the drop-down list.
 - Port—Port Number of the CiscoWorks server.

If the DCR Master (local server) is in ACS mode, you should enter the Network Device Group (NDG) details.

This should be the NDG to which the DCR Master server is added. CiscoWorks Assistant will convert the server you add here into ACS mode, after the Manage Servers workflow has successfully completed.

After the workflow has successfully completed, if the server you are adding has already been integrated with another ACS server, it will get integrated to the ACS server to which the DCR Master (local server) is integrated.

If you add a server that is already registered with the same ACS server as the DCR Master (local server), CiscoWorks Assistant re-integrates the server with the same ACS server.

After integration, all custom roles that you have created in the ACS server for the CiscoWorks applications will be lost.

You must restart the Daemon Manager in the server that you have added, after the Manage Server Step is complete. If you have added multiple servers, you must restart the Daemon Manager in all servers that you have added.

If the DCR Master is in CiscoWorks Local mode, you cannot add a server that is in ACS mode.

Step 4 Click **Next** to continue.

CiscoWorks server is contacted to validate the Device and Credential Repository settings, and to fetch the Certificate information.

For more information on this, see the Online Help or the *User Guide for CiscoWorks Assistant 1.1*.

Set up Device Management Mode For Applications in All Servers

You can set up the device management mode of all applications in DCR Master and one or more DCR Slave servers from the DCR Master machine.

Setting up the device management mode for a multi-server setup is similar to the process followed in a single-server setup. See [Set up Device Management Mode](#) and perform the steps as indicated here.

Set up Default Credentials in DCR Master

Setting up the default credentials for a multi-server setup is similar to the process followed in a single-server setup. See [Set up Default Credentials](#) and perform the steps as indicated here.

You can set up Default Credentials only in DCR Master server.

Add Devices to DCR

Adding devices to the DCR for a multi-server setup is similar to the process followed in a single-server setup. See [Add Devices](#) and perform the steps as indicated here.

You can add devices to DCR using the Bulk Import From File and Bulk Import From NMS options only from DCR Master server.

Manage Devices in the Applications Installed in All DCR Servers

You can select devices from the device selector and add it to the application with which you want the device to be managed in a multi-server setup. It is similar to the process followed in a single-server setup. See [Manage Devices in the Applications Installed in the LMS Servers](#) and perform the steps as indicated here.

The Server Setup Summary page appears at the end with a summary of Session details, Server Summary and the Operational details. For more details, see the Viewing Server Addition Summary section in the *User Guide of CiscoWorks Assistant 1.1*.

Integrating CiscoWorks Server with ACS

CiscoWorks login modules allow administrators to add new users using a source of authentication other than the native CiscoWorks Server mechanism (that is, the CiscoWorks Local login module). You can use Cisco Secure ACS services for this purpose.

This section explains the following:

- [CiscoSecure ACS Support](#)
- [CiscoWorks Server Authentication Roles](#)
- [Before You Begin ACS Integration](#)
- [Setting Up ACS Server](#)
- [Changing the AAA Mode to ACS Using the Server Setup Workflow](#)
- [Assigning Roles to Users and User Groups In ACS](#)
- [Impact of Installing CiscoWorks Applications in ACS Mode](#)
- [Verifying LMS Applications and the Cisco Secure ACS Configuration](#)

CiscoSecure ACS Support

CiscoWorks Common Services supports ACS mode of authentication and authorization.

To use this mode, you must have a Cisco Secure ACS (Access Control Server), installed on your network. Common Services 3.2 supports the following versions of Cisco Secure ACS:

- Cisco Secure ACS 3.2 for Windows Server
- Cisco Secure ACS 3.2.3 for Windows Server
- Cisco Secure ACS 3.3.2 for Windows Server
- Cisco Secure ACS 3.3.3 for Windows Server
- Cisco Secure ACS 3.3.4 for Windows Server
- Cisco Secure ACS 4.0.1 for Windows Server
- Cisco Secure ACS 4.1 for Windows Server
- Cisco Secure ACS 4.1.1 for Windows Server
- Cisco Secure ACS 4.1.4 for Windows Server
- Cisco Secure ACS 4.2 for Windows Server
- Cisco Secure Appliance 3.3.3
- Cisco Secure Appliance 3.3.4
- Cisco Secure Appliance 4.0.1
- Cisco Secure Appliance 4.1
- Cisco Secure Appliance 4.1.1
- Cisco Secure Appliance 4.1.4
- Cisco Secure Appliance 4.2

We recommend that you install the Admin HTTPS PSIRT patch, if you are using ACS 3.2.3.

To install the patch:

-
- Step 1** Go to <http://www.cisco.com/pcgi-bin/tablebuild.pl/cs-ac-win>.
You must enter Cisco.com username and password after you launch this URL.
- Step 2** Click the Download CiscoSecure ACS Software (Windows) link.
You can find the link to the Admin HTTPS PSIRT patch, in the table.
-

CiscoWorks Server Authentication Roles

By default, the CiscoWorks server authentication provides the following roles. They are listed here from least privileged to most privileged:

1. Help Desk
2. Approver
3. Network Operator
4. Network Administrator
5. System Administrator
6. Super Admin (in ACS mode and on ACS Server only)



Note

See *User Guide for CiscoWorks Common Services 3.2* for information about CiscoWorks Server Authentication Roles.

The CiscoWorks Server provides the Super Admin role in ACS mode. This role can perform all CiscoWorks operations including the administration and approval tasks.

You cannot assign a local user with this role. You can assign this role to a user only on CiscoSecure ACS Server and only when your login module is set to ACS. This role is not visible in CiscoWorks local mode and during the local user setup in CiscoWorks Server.

We recommend that you do not modify the default CiscoWorks roles. However, you can create your own custom roles on Cisco Secure ACS. See [Assigning Roles to Users and User Groups In ACS](#) for more information.

For more information, see *User Guide for CiscoWorks Common Services 3.2*.

Before You Begin ACS Integration

Before you integrate the CiscoWorks Server with ACS, ensure that you:

1. Set up a System Identity User in CiscoWorks Server

You can either use the Common Services or the CiscoWorks Assistant Server Setup workflow to configure a System Identity User.

2. Assign all the local user privileges to System Identity User in CiscoWorks Server

You should add the System Identity User as a local user and assign all the privileges in CiscoWorks Server.

See the Setting up Local Users section in *User Guide for CiscoWorks Common Services 3.2* to configure System Identity User configured as a local user and assign all privileges in CiscoWorks Server.

If System Identity User is not configured with all local user privileges, authorization fails when you try perform certain tasks in CiscoWorks Server.

Setting Up ACS Server

You should perform the tasks in ACS before you change the AAA mode of CiscoWorks Server to ACS.

1. Configure ACS Administrators in ACS Server

You should configure the ACS administrators with all privileges in ACS. The ACS administrator account in ACS is required to:

- Access the ACS server from any remote machine.
- Enter the login details during the AAA mode setup in Common Services.

Only then does authentication occur from the ACS Server.

Also, if you do not configure the ACS administrative user with all the privileges, the application registration with ACS will fail.

2. Create a Network Device Group

Network Device Groups (NDGs) are collection of AAA clients such as servers and network devices.

You should add the group of servers and network devices only under a NDG. You can use the existing NDGs or you can create a new NDG for this purpose.

If you want to use an existing NDG, this step is optional.

3. Add CiscoWorks Server and Network Devices as AAA Clients

You should configure the following as AAA Clients in ACS Server:

- CiscoWorks Server

You should manually add the DCR Master server as an AAA client in ACS, before you change the mode to ACS.

When you use CiscoWorks Assistant Server Setup workflow, the workflow converts the AAA mode of other servers in the multi-server setup to ACS mode.

- Devices managed by CiscoWorks Server

You should add the devices managed by CiscoWorks in ACS after you have configured the CiscoWorks Server as a AAA client.

If you do not configure the devices as AAA clients in ACS, the devices will not be visible in CiscoWorks Server after the integration.

If you use CiscoWorks Assistant Server Setup workflow to change the AAA mode to ACS, the missing devices are added to the NDG you specify.

4. Configure the CiscoWorks Administrative Users in ACS

You should add CiscoWorks System Identity User and other CiscoWorks administrators in ACS. Otherwise if you log in as a user configured only in Common Services, authentication will not happen.

You can create a user group in ACS and add all users to that user group.

See the following documents on Cisco.com for details how to perform each of the above tasks:

- *User Guide for Cisco Secure Access Control Server 3.x and 4.x*
http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html
- *User Guide for CiscoWorks Common Services 3.2*
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html
- *CiscoWorks LMS Integration with Cisco Secure ACS whitepaper*
http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_white_papers_list.html

Changing the AAA Mode to ACS Using the Server Setup Workflow

To change the mode to ACS:

Step 1 Select **CiscoWorks Assistant > Workflows > Server Setup > Change ACS Setup**.

CiscoWorks Assistant checks whether there are pending devices in DFM and RME. If CiscoWorks Assistant finds any pending devices, the Pending Device Count table is displayed with the following details:

- Server—Server name.
- Application—The application that contains pending devices. The values will be DFM or RME.
- Pending Count—Number of pending devices.
- Details—The reason why CiscoWorks Assistant could not fetch the pending device count. This column will be blank if the pending devices count is found.

Along with the table, a Notification pop up window appears with the following message:

Pending devices exist or could not check for pending devices in some LMS applications

Step 2 Click **OK**.

Step 3 Click **Next**.

A confirmation pop up appears with the following message:

LMS server(s) ACS configuration will not be proper if there are pending devices in the LMS applications. Make sure there are no pending devices and click OK to continue.

To get further details on pending devices in the applications, go to:

- **RME > Devices > Device Management > Pending Devices**
- **Device Fault Manager > Device Management > Device Summary**

See RME and Device Fault Manager User Guides for more information on pending devices.

Step 4 Click **OK**.

The Change ACS Setup page appears.

Step 5 Select the Change Mode to ACS check box and click **Next** to go the Configure ACS Mode page.**Note**

Ensure that the local server is an AAA client to ACS server.

Step 6 Click **OK** on the Notification pop-up window to continue with the ACS Mode change.**Step 7** Enter the required information in the ACS Mode Setup table to change the login mode to ACS.

If the DCR Master (local server) is already in ACS mode, the fields other than the passwords and secret keys will be pre-populated.

Step 8 Select **Register all installed applications with ACS**, if you are registering the applications for the first time.

In case an application is already registered with ACS, the current registration will overwrite the previous registration.

When you select the Register all installed applications with ACS check box, you are prompted to confirm whether you want to continue with the settings.

See Common Services Online Help for details.

Step 9 Select the HTTP or HTTPS radio button under Current ACS Administrative Access Protocol.**Step 10** Click **Next** to complete the mode change.

The Configure ACS Mode Progress page is displayed. You can view the ACS mode configuration status in this page.

**Note**

Restart Daemon Manager after you configure ACS Mode for the changes to take effect.

Assigning Roles to Users and User Groups In ACS

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.

You can either:

- Assign predefined roles to CiscoWorks Users in ACS.

Or

- Create custom roles and assign them to CiscoWorks Users in ACS.

You ensure that the CiscoWorks user or the user group has been assigned the proper privileges in ACS mode. You can assign a desired role to the user or user group, or assign roles on an NDG basis.

See the following topics in *User Guide for CiscoWorks Common Services 3.2* for more information:

- Roles in ACS
- Assigning Roles to Users and User Groups in ACS

Impact of Installing CiscoWorks Applications in ACS Mode

We recommend that you integrate CiscoWorks server and Cisco Secure ACS after installing all of the LAN Management Solution applications.

If you install any application on the CiscoWorks Server when AAA mode is set to ACS, you might be prompted with a message to re-register the application with ACS.

For example, if you have integrated CiscoWorks server and Cisco Secure ACS before installing any application, you are prompted with this message at the time of installation of the selected application:

CiscoWorks Server is in ACS mode

The application that you are installing requires new tasks to be registered with ACS. If you have already registered this application with ACS from another server, you do not need to register it again. However if you re-register the application, you will lose any custom roles that you had created earlier for this application in ACS.

Enter (Y)es to Register, (N)o to continue without registering,

(Q)uit: [N]

- If you enter **Y**, the application gets registered with ACS server.
- If you enter **N**, the application does not get registered with ACS server.

After installation, you can register RME 4.2 with ACS server, using the **AcsRegCli.pl** script:

```
/opt/CSCOpX/bin/perl /opt/CSCOpX/bin/AcsRegCli.pl -register rme
```

When you re-register, the custom roles you have created may be lost.

- If you have installed your application after configuring the CiscoWorks Login Module to ACS mode, the application users are not granted any permission.

However, the application is registered to the Cisco Secure ACS. On the Cisco Secure ACS server, you must assign the appropriate permissions to the application.

- Multiple instances of same application using same Cisco Secure ACS will share settings. Any changes will affect all instances of that application.
- If application is configured with Cisco Secure ACS and then the application is reinstalled, the application will inherit the old settings.

Verifying LMS Applications and the Cisco Secure ACS Configuration

After performing the above mentioned tasks on Cisco Secure ACS server, login to CiscoWorks with the username as defined in the Cisco Secure ACS.

Based on your privilege on the Cisco Secure ACS, you can perform only certain tasks on the CiscoWorks Server.

For example, if your privilege is of Help Desk, you can only view the Device Summary.

You can view only certain devices in the CiscoWorks Server. This depends on the Network Device setting for the User/Group on the Cisco Secure ACS.

Managing Devices in CiscoWorks Server

This section contains the following:

- [Managing Devices and Credentials](#)
- [Managing Devices in CiscoWorks Applications](#)

Managing Devices and Credentials

You can also add devices to DCR using the Device Management page (**Common Services > Device and Credentials > Device Management**).

You can use the Device and Credential Repository Administration to:

- Edit device identity
- Edit device credentials
- Import bulk devices
- View the list of devices on CiscoWorks Server
- Export devices
- Exclude devices
- Delete devices

You can use the device selector to search and select the devices for performing device management tasks.

For more information on the Device and Credential Repository, see the Online Help or the *User Guide for CiscoWorks Common Services 3.2*.

Managing Devices in CiscoWorks Applications

You can manage the devices and allocate them to be managed by the applications installed in the CiscoWorks servers.

See the following sections for information on managing devices in CiscoWorks applications using CiscoWorks Assistant.

- [Device Management Modes](#)
- [Setting Up a Single CiscoWorks Server](#)
- [Setting Up Multiple CiscoWorks Servers](#)

Apart from the device management tasks you perform as part of CiscoWorks Assistant Server Setup, you can manage the devices in the applications.

See [Table 5-4](#) to understand about:

- Default Device Management modes of CiscoWorks applications.
- Brief description on how to change the device management mode and manage devices in the applications.

Additionally, you can manage the devices in:

- RME, using `cwcli` Inventory Command. See [RME Device Management Using cwcli Inventory Command](#).
- IPM, using Adhoc Target Devices. See [Adding Adhoc Target Devices to IPM](#).

RME Device Management Using cwcli Inventory Command

The `cwcli` inventory is a RME Device Management application command line tool. It allows you to:

- Check the specified device credentials for the RME devices.
- Export device credentials of one or more RME devices in clear text.
- Delete the specified RME devices.
- View the RME devices state.

The `cwcli inventory` command is located in the following directories, where `install_dir` is the directory in which CiscoWorks is installed:

- On Solaris systems, `/opt/CSCOpX/bin`
- On Windows systems, `install_dir\CSCOpX\bin`

The default install directory is `System_Drive:\Program Files`.

For more detailed information on this, refer the Online Help or see the *User Guide for Resource Manager Essentials 4.2*.

Adding Adhoc Target Devices to IPM

You can add adhoc target devices from the IPM Devices page other than managing the devices automatically or manually in IPM (**Internetwork Performance Monitor > Collector Management > Devices**).

For more detailed information on this, see the *User Guide for Internetwork Performance Monitor 4.1*.

Preparing to Use LMS Applications

You must perform some configuration activities in few applications to get started with them to be able to use the functions they provide.

The following are some of the important configuration operations you must perform.

This section contains:

- [Preparing to Use Campus Manager](#)
- [Preparing to Use Device Fault Manager](#)
- [Preparing to Use Internetwork Performance Monitor](#)
- [Preparing to Use Resource Manager Essentials](#)
- [Preparing to Use Health and Utilization Monitor](#)
- [Using CiscoView](#)
- [Using Device Center](#)
- [Using Integration Utility](#)

Preparing to Use Campus Manager

The following sections will help you prepare to use Campus Manager:

- [Processes and Settings](#)
- [Data Collection Settings](#)
- [User Tracking Settings](#)
- [Starting Topology Services](#)
- [Configuring SNMP Trap Listener for Dynamic UT to Work in Campus](#)

For details on the new features introduced in Campus Manager 5.1, see the Whats New section in the *User Guide for Campus Manager 5.1*.

Processes and Settings

The following are the two main processes in Campus Manager:

- Data Collection

Fetches the device list from DCR and collects the following data from the network:

- Ports available in a device
- VLANs present in the network/ device
- Subnets in the network
- Discrepancies in the network
- Neighbor data for each device
- Details about STP running in the network

- User Tracking Major Acquisition

The data collected by the above processes is used by Campus Manager to generate reports about the network.

Data Collection Settings

Using the Data Collection option, you can:

- Specify the time period at which SNMP queries time out, and the number of retries that can be attempted by Campus Manager before it stops querying the device.
- Include or exclude devices for Data Collection by setting appropriate filters.
- Schedule the time intervals at which Data Collection runs.

You can configure the Device Discovery Settings, either using LMS Setup Center or using Campus Manager Administration.

Go to **Campus Manager > Admin > Data Collection** and configure these settings. See *User Guide for Campus Manager 5.1* for more information.

User Tracking Settings

You can configure the following options based on which data on end-hosts and IP phones in the network are collected:

- Acquisition Settings

Before you start collecting information about the hosts in your network, you can set various options that control the way in which Acquisition happens.

For example, you can set Campus Manager to perform DNS lookup, while resolving the IP address of a host.

- Schedule Acquisition

You can set the day and time of the week when you want to run Major Acquisition. The time interval at which Minor Acquisition happens in the network can also be set.

- Specifying Report Purge Policy

You can specify the intervals when you want old reports and jobs to be purged. You can save the Purge Policy, so that the older jobs and archives are purged at the specified intervals.

- Specifying Report Domain Name Display

You can specify the way in which domain names are displayed in User Tracking Reports.

- Configuring Ping Sweep Options For UT Acquisition

You can configure Campus Manager to perform Ping Sweep on selected subnets, during Acquisition.

- Configuring Subnet Acquisition

You can trigger acquisition on a single subnet or a select set of subnets. Subnet based acquisition collects details about the end hosts that are connected to a particular subnet or a select set of subnets. This Acquisition completes faster, since it is not run on all devices managed by Campus Manager.

- Configuring End Host and IP Phone Data Delete Interval

You can modify the time interval for deleting entries from the End Host Table, IP Phone Table, or the History Table from the database.

- Importing Information on End Hosts

You can import user names and notes for end hosts that are already discovered by User Tracking, from a file.

- Enabling Dynamic User Tracking

Dynamic Updates are asynchronous updates that are based on SNMP MAC notifications traps. Campus Manager tracks changes about the end hosts and users on the network to provide real-time updates, based on these traps.

Go to **Campus Manager User Tracking > Administration** from the Campus Manager home page to configure the User Tracking Settings.

See *User Guide for Campus Manager 5.1* for more information.

Starting Topology Services

You must install the Java plug-in to access Topology Services from a client. If you are prompted to install the Java plug-in, download and install it using the installation screens displayed. The next time you start the application, it automatically uses the plug-in.

Launching Topology Services From Solaris Client

The Topology_Services.jnlp file has to be associated with the correct Java application for Topology services to launch properly. You need to associate the jnlp file only once, when you access Topology Services for the first time.

To associate the jnlp file with the correct Java application:

-
- Step 1** Select **Campus Manager > Visualization > Topology Services** from LMS Portal.
A popup window displays prompting you to save or cancel Topology_Services.jnlp file.
 - Step 2** Click **Save**.
 - Step 3** Go to the folder where you saved the file, right -click the file and choose **Open with**.
A popup window appears.
 - Step 4** Click **Go here**.
Another popup window appears.
 - Step 5** Click **Browse** and locate the jre folder.
For example, if your Java plugin version is jre1.6.0_05, the directory can be /usr/java/jre1.6.0_05/bin
 - Step 6** Associate the file with javaws, by choosing javaws from the above path.
 - Step 7** Click **Apply** and close the pop up window.
 - Step 8** Click on the Topology_Services.jnlp file to launch Topology services.
-

Configuring SNMP Trap Listener for Dynamic UT to Work in Campus

Before you start using this application, you should configure the SNMP Trap Listener for Dynamic UT to work in Campus Manager.

User Tracking Dynamic Updates tracks changes of the end hosts and users in the network with minimal time delay. In addition to polling the network at regular intervals, Campus Manager tracks the changes in the network whenever they occur.

In Dynamic UT, the devices send traps to Campus Manager whenever changes occur in the network. This implies that you need not wait till next UTMajor Acquisition cycle to see the changes that have happened in your network.

As a result of Dynamic updates, the following reports contain the latest information:

- End-Host Report - Contains information from UT Major Acquisition and the recently added end-hosts.
- History Report - Contains information from UT Major Acquisition and the recently disconnected end-hosts/end-hosts that have moved between ports or VLANs.
- Switch Port reports - Contains information about the utilization of switch ports.

SNMP Traps are generated when a host is connected to the network, disconnected from the network or when it moves among VLANs or ports in the network.

To enable Dynamic Updates feature, switches must be managed by Campus Manager.

You must configure Campus Manager as a primary or secondary receiver of the MAC notifications.

You must also configure SNMP Trap Listener. To do this:

-
- Step 1** Select **Campus Manager > Administration** from CiscoWorks home page.
- Step 2** Select **Dynamic Updates > Trap Listener Configuration**.
The Trap Listener Configuration dialog box appears.
- Step 3** Check **Listen traps from Device** to configure the trap reception directly from the devices.
or
Check **Listen traps from DFM/HPOV** to receive the traps through these applications.
- Step 4** Enter the port number of the port through which you want to receive the traps, in the Trap Listener Port field.
The default trap listener port number of the Campus Manager server is 1431.
- Step 5** Click **Apply** to save the details.
-

- Configure all devices to send traps to the Trap Listener port of the Campus Manager server. This is the port number that you would have configured on Campus Manager Administration screen.
For more information, see the Online Help or see the Enabling SNMP Traps on Switch Ports section in the *User Guide for Campus Manager 5.1*.
- Configure DHCP snooping on the switches.
For more detailed information on this, see the Administering Campus Manager section in the *User Guide for Campus Manager 5.1*.

Preparing to Use Device Fault Manager

This section contains:

- [Enabling Devices to Send Traps to DFM](#)
- [Integrating DFM Trap Receiving with NMSs or Trap Daemons](#)
- [Updating the SNMP Trap Receiving Port](#)
- [Configuring SNMP Trap Forwarding](#)

DFM can receive traps on any available port and forward them to other NMSs (specified by IP addresses and ports). This capability enables DFM to easily work with other trap processing applications.

DFM will only forward SNMP traps from devices in the DFM inventory. It will not change the trap format. It will only forward the raw trap in the format in which the trap was received from the device.

However, you must enable SNMP on your devices and you must do one of the following:

- Configure SNMP to send traps directly to DFM
- Integrate SNMP trap receiving with an NMS or a trap daemon

To send traps directly to DFM, perform the tasks in [Enabling Devices to Send Traps to DFM](#).

To integrate SNMP trap receiving with an NMS or a trap daemon, follow the instructions in [Integrating DFM Trap Receiving with NMSs or Trap Daemons](#).

For details on the new features introduced in DFM 3.1, see the Whats New section in the *User Guide for Device Fault Manager 3.1*.

Enabling Devices to Send Traps to DFM

Since DFM uses SNMP MIB variables and traps to determine device health, you must configure your devices to provide this information.

For any Cisco devices that you want DFM to monitor, SNMP must be enabled and the device must be configured to send SNMP traps to the DFM server.

Make sure your devices are enabled to send traps to DFM. You can verify whether the devices are enabled using the command line or GUI interface appropriate for your device. This is explained in the following sections:

- [Enabling Cisco IOS-Based Devices to Send Traps to DFM](#)
- [Enabling Catalyst Devices to Send SNMP Traps to DFM](#)

Enabling Cisco IOS-Based Devices to Send Traps to DFM

For devices running Cisco IOS software, enter the following commands:

```
(config)# snmp-server [community string] ro
(config)# snmp-server enable traps
(config)# snmp-server host [a.b.c.d] traps [community string]
```

where *[community string]* indicates an SNMP read-only community string and *[a.b.c.d]* indicates the SNMP trap receiving host (the DFM server).

For more information, see the appropriate command reference guide.

To enable the devices to send traps to DFM:

-
- | | |
|---------------|---|
| Step 1 | Log into Cisco.com. |
| Step 2 | Select Products & Solutions > Cisco IOS Software . |
| Step 3 | Select the Cisco IOS Software release version used by your Cisco IOS-based devices. |
| Step 4 | Select Technical Documentation and select the appropriate command reference guide. |
-

Enabling Catalyst Devices to Send SNMP Traps to DFM

For devices running Catalyst software, enter the following commands:

```
(enable)# set snmp community read-only [community string]
(enable)# set snmp trap enable all
(enable)# set snmp trap [a.b.c.d] [community string]
```

Where *[community string]* indicates an SNMP read-only community string and *[a.b.c.d]* indicates the SNMP trap receiving host (the DFM server).

For more information, see the appropriate command reference guide.

To enable the devices to send traps to DFM:

-
- | | |
|---------------|---|
| Step 1 | Log in to Cisco.com. |
| Step 2 | Select Products & Solutions > Switches . |
| Step 3 | Select the appropriate Cisco Catalyst series switch. |
| Step 4 | Select Technical Documentation and select the appropriate command reference guide. |
-

Integrating DFM Trap Receiving with NMSs or Trap Daemons

You might need to complete one or more of the following steps to integrate SNMP trap receiving with other trap daemons and other Network Management Systems (NMSs):

- If you are integrating DFM with a remote version of HP OpenView or NetView, you must install the appropriate adapter on the remote HP OpenView or NetView. You do not need to install any adapters if HP OpenView or NetView is installed locally. For more information on this, see the *User Guide for Device Fault Manager*.
- Add the host where DFM is running to the list of trap destinations in your network devices. See [Enabling Devices to Send Traps to DFM](#).
Specify port 162 as the destination trap port. (If another NMS is already listening for traps on the standard UDP trap port (162), use port 9000, which DFM will use by default.)
- If your network devices are already sending traps to another management application, configure that application to forward traps to DFM.

**Note**

For integration of DFM with HP OpenView or NetView, it is suggested that you install HPOV/NetView before installing LMS.

Table 5-6 describes scenarios for SNMP trap receiving and lists the advantages of each.

Table 5-6 Configuring Scenarios For DFM Trap Receiving

Scenario	Advantages
Network devices send traps to port 162 of the host where DFM is running. DFM receives the traps and forwards them to the NMS.	<ul style="list-style-type: none"> • No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • DFM provides a reliable trap reception and forwarding mechanism. • NMS continues to receive traps on port 162. • Network devices continue to send traps to port 162.
The NMS receives traps on default port 162 and forwards them to port 162 on the host where DFM is running.	<ul style="list-style-type: none"> • No reconfiguration of the NMS is required. • No reconfiguration of network devices is required. • DFM does not receive traps dropped by the NMS.

Updating the SNMP Trap Receiving Port

By default, DFM receives SNMP traps on port 162 (or, if port 162 is occupied, port 9000). If you need to change the port, you can do so. DFM supports SNMP V1, V2, and V3 traps for trap receiving (although DFM only supports authNoPriv for V3 traps).

-
- Step 1** Select **Configuration > Other Configurations > SNMP Trap Receiving** from the configuration tab of the DFM home page.
- Step 2** Enter the port number in the Receiving Port entry box.
- Step 3** Click **Apply**.
-

See [LAN Management Solution Port Usage](#) for information of port that are already in use. If you have two instances of the DfmServer process running, traps will be forwarded from the first instance to the second instance.

Configuring SNMP Trap Forwarding

DFM will only forward SNMP traps from devices in the DFM inventory. DFM will not change the trap format. It will forward the raw trap in the format in which it was received from the device. All traps are forwarded in V1 format.

-
- Step 1** Select **Configurations > Other Configurations > SNMP Trap Forwarding** from the Configuration tab of the DFM home page.
- Step 2** For each host, enter:
- An IP address or DNS name for the hostname.
 - A port number on which the host can receive traps.
- Step 3** Click **Apply**.
-

Preparing to Use Internetwork Performance Monitor

The following sections explain you how to get started and work with Internetwork Performance Monitor.

- [IPM Application Settings](#)
- [Auto Allocation Settings](#)
- [Managing IPM Operations](#)
- [Working With Collectors](#)

For details on the new features introduced in IPM 4.1, see the Whats New section in *User Guide for Internetwork Performance Monitor 4.1*

IPM Application Settings

You can perform the application setup tasks in the Application Settings page.

Select **Internetwork Performance Monitor > Admin > Application Settings** to launch this page.

The following are the application setup tasks in IPM:

- Copy IPSLA Configuration to running-config.

You can see the IP SLA (Internet Protocol Service Level Agreement) probes for the collectors that you configure in IPM at the command line interface of the router in the running configuration.

It does this by selecting the Copy IP SLA Configuration to running-config option on the Application Settings page.

This option is not selected by default. You cannot view the IP SLA probes in the running configuration of the source router if this option is not set.

**Note**

The IP SLA probes are automatically reconfigured when you reboot if you have selected this option and saved the IP SLA probes of the IPM collectors in the startup configuration.

- Use Managed Source Interface Address

Managed Source Interface configures the source router with the appropriate IP address for sending or receiving the IP SLA (Internet Protocol Service Level Agreement) operation packets.

You can set a source interface address for the source router by selecting the Use Managed Source Interface Address option on the Application Settings page. After this option is set, the source router uses the managed interface address while configuring the collectors on the source device.

However, you can also specify a source interface address while configuring a collector. In that case, the source router uses the specified interface.

If the Use Managed Source Interface option is not set, then by default, the source router selects the source interface for the collector from the Routing Table, based on the IP address of the destination.

For more information on this, see the Online Help or see the *User Guide for Internetwork Performance Monitor 4.1*.

Auto Allocation Settings

Before adding devices to IPM, you can use the Auto Allocation Settings option to enable automatic allocation of devices to IPM from Device Credentials Repository (DCR).

To change the device management settings, go to LMS Portal and select **Internetwork Performance Monitor > Admin > Auto Allocation Settings**.

The Auto Allocation Settings page consists of the following settings:

- Enable Auto Mode

Automatically adds all devices that are added into DCR, to IPM, as well.

Since this option is disabled by default, you must enable it if you want to automatically add devices to IPM. The number of devices added into IPM depends on the license limit.

- Manage All Devices

Allows you to add devices from DCR and manage them in IPM.

This allocation method is dynamic. The devices added to DCR after applying this setting, are also added into IPM at runtime. The number of devices added into IPM depends on the license limit.

You can use this option only if you have checked Enable Auto Mode. If you select this option and you delete a device from DCR, the device is also deleted from IPM.

- Manage By Groups

Allows you to add devices from DCR and manage them in IPM, based on groups. The devices that are part of the selected groups, are added into IPM.

This allocation method is dynamic. The devices added to DCR after applying this setting, are also added into IPM at runtime. The number of devices added into IPM, depends on the license limit.

You can use this option only if you have selected Enable Auto Mode.

- Group Selector

Lists the groups available for Auto Allocation. Select one or more groups so that devices in those groups are added into IPM automatically.

You can use this option only if you have checked Enable Auto Mode.

- Devices that do not Match the Policy

Allows you to generate a report for devices that are managed by IPM but do not satisfy the grouping rule criteria.

You can use this option only if you have selected Manage By Groups.

For more information on this, see the Online Help or see the *User Guide for Internetwork Performance Monitor 4.1*.

Managing IPM Operations

IPM supports the following IP SLA operations:

- Echo Operations
 - Echo
 - Path Echo
 - UDP Echo (User Data Protocol)

- Jitter Operations
 - ICMP Jitter (Internet Control Message Protocol)
 - UDP Jitter (User Data Protocol)
- VoIP Operations
 - Call Setup Post Dial Delay
 - Gatekeeper Registration Delay
 - RTP (Real-time Transfer Protocol)
- Operation based on Services
 - DNS (Domain Name System)
 - DHCP (Dynamic Host Configuration Protocol)
 - HTTP (HyperText Transfer Protocol)
 - FTP (File Transfer Protocol)
 - DLSw (Data-link Switching)
 - TCP Connect
- Metro Ethernet Operations
 - Ethernet Ping
 - Ethernet Jitter
 - Ethernet Ping Auto IP SLA
 - Ethernet Jitter Auto IP SLA

When you install IPM, a group of predefined operations are provided. You can define one or more new operations to suit your needs. Although, you cannot modify the default operations, you can use them as templates for your own operations.

You can perform the Operation management tasks using the IPM Operation Management page.

To launch this page, go to **Internetwork Performance Monitor > Collector Mgmt > Operations**.

The various Operation management tasks include:

- Viewing the details of predefined or user-defined operations
- Creating user-defined operations
- Editing user-defined operations
- Deleting user-defined operations
- Filtering the list of operations displayed based on certain filtering criteria

See *User Guide for Internetwork Performance Monitor 4.1* for more information.

Working With Collectors

The Collector Configuration page in Internetwork Performance Monitor (IPM) allows you to configure collectors. You can configure collectors by specifying the collector information, a source device, target devices, and operations.

The number of collectors you create in IPM depends on your device license. The IPM Collector license limit applies only to historical collectors and not to real-time collectors. You are allowed to create real-time collectors even after the license limit is reached.

However, we recommend that you create collectors based on the polling interval for better performance of the IPM server.

To create collectors:

Step 1 Go to the LMS Portal and select **Internetwork Performance Monitor > Collector Management > Collectors**.

The Collector Management page appears.

Step 2 Click **Create**.

The Collector Configuration page appears.

Step 3 Specify the following details in the Collector Info section:

- The collector name in the Collector Name field.
- A brief description of the collector in the Description field.

Though the Collector Name field allows you to enter more than 15 characters, the Source device and trap PDUs display only the first 15 characters for the IOS version.

The IPM database, however, will contain the complete collector name you have entered.

Step 4 Select the source router from the Source Devices list.

Step 5 Select one or more target devices from the Target Devices list.

Step 6 Select one or more operations from the Operations list.

Step 7 Enter a valid IP address in the Source Interface field. This is optional.

This is the IP address of the source device interface to which the packets are returned from the destination. The Source Interface field is an optional field.

Step 8 Click **Next**.

Step 9 The Select Collector page appears.

You can then select the collectors and perform various functions such as scheduling, viewing collector summary, editing collectors, importing and exporting collectors that helps you manage these collectors effectively.

For more information on this, see the Online Help or see the *User Guide for Internetwork Performance Monitor 4.1*.

Preparing to Use Resource Manager Essentials

The following sections help you to get started with Resource Manager Essentials:

- [Setting Up Inventory](#)
- [Setting Up Syslog Analyzer](#)
- [Setting Up Software Management](#)
- [Setting Up Configuration Management](#)

Several important items must be configured correctly on every Cisco device that will be managed and monitored through RME. See [Required Device Credentials for LMS Applications](#) for information on the required device credentials for RME applications.

For details on the new features introduced in RME 4.2, see the Whats New section in the *User Guide for Resource Manager Essentials 4.2*.

Setting Up Inventory

This section describes the tasks that you must perform to set up the Inventory application.

To set up RME Inventory, you should perform the following tasks:

- Create network inventory by either adding device information by adding one device at a time or performing Bulk Import from DCR.
- Obtain the login privileges to Cisco.com. See [Logging Into Cisco.com for Software Management Tasks](#) for more information.
- Schedule inventory polling and collection.
- Set change report filters.
- Display a detailed device report
- Set Cisco.com Fetch Interval.

See *User Guide for Resource Manager Essentials 4.2* for more information.

Setting Up Syslog Analyzer

In RME, you should configure the devices to send Syslogs before starting to use this application.

The Syslog Analyzer allows you to centrally log and track Syslogs (such as system error messages, exceptions, and other information such as device configuration changes etc.) from devices, that you can use to analyze device and network performance.

You must configure devices to forward messages to the RME server or to a system on which you have installed the Common Syslog Collector.

Before you can use Syslog Analyzer, you must configure devices to forward messages to RME or a system on which you have installed the distributed Syslog Analyzer Collector.

For more information about setting up devices for message logging, see the Syslog Online help, the Cisco IOS Software Documentation on Cisco.com (for Cisco IOS devices), and the appropriate guides.

To configure the device using Telnet, perform the tasks for each type of devices:

- [IOS Devices](#)
- [Catalyst Devices](#)

See *User Guide for CiscoWorks Resource Manager Essentials 4.2* for details on how to configure the other device types using Telnet.

IOS Devices

To configure IOS devices using Telnet:

-
- Step 1** Connect to the device using Telnet and log in.
The prompt changes to `host`.
- Step 2** Enter **enable** and the enable password.
The prompt changes to `host#`.
- Step 3** Enter **configure terminal**.
You are now in configuration mode, and the prompt changes to `host(config)#`.
- To make sure logging is enabled, enter **logging on**.
 - To specify the RME server to receive the router Syslog messages, enter **logging IP address**, where *IP address* is the server IP address.
 - To limit the types of messages that can be logged to the RME server, enter **logging trap informational** to set the appropriate logging trap level by, where *informational* signifies severity level 6.

This means all messages from level 0-6 (from emergencies to informational) will be logged to the RME server.

Catalyst Devices

To configure Catalyst devices using Telnet:

-
- Step 1** Connect to the device using Telnet and log in.
The prompt changes to `host`.
- Step 2** Enter **enable** and the enable password.
The prompt changes to `host#`.
- To make sure logging is enabled, enter **set logging server enable**.
 - To specify the RME server that is to receive the Catalyst devices Syslog messages, enter **set logging server IP address**, where *IP address* is the server IP address.
 - To limit the types of messages that can be logged to the RME server, enter **set logging level all 6 default**.

This means that all messages from level 0-5 (from emergencies to notifications) will be logged to the RME server.

See the appropriate Catalyst reference manual for more information.

For more information on this, see the Online Help or the *User Guide for Resource Manager Essentials 4.2*.

Setting Up Software Management

Software Management application performs system software upgrades, boot loader upgrades, and software configuration operations on groups of routers and switches.

Before you can use Software Management, you must have sufficient space to store the software image files. Depending upon the software image, you should have 4 MB to 150 MB of free space.

To set up Software Management, you must:

- Set up File Transfer Servers

The supported protocols for image import or distribution are rcp, TFTP, SCP and HTTP. The file transfer servers that the Software Management application uses to transfer software files are installed by Common Services.

- Set Software Management Preferences

Select **Resource Manager Essentials > Admin > Software Mgmt > View/Edit Preferences** to set your Software Management Preferences such as image distribution, import and so on.

- Create a baseline of the devices in your network and populate the software image library.

To do this, go to **Resource Manager Essentials > Software Mgmt > Software Repository** and click **Add** and select **Device**.

- Schedule the Synchronize Library job to run periodically.

To do this, go to **Resource Manager Essentials > Software Mgmt > Software Repository > Software Repository Synchronization**.

- Create one or more approver lists if you want to use the Job Approval option.

To enable Job Approval, use **Resource Manager Essentials > Admin > Approval**.

- Distribute a software image to a device or group of devices

Depending on system complexity, you can configure upgrades for groups of devices to the same software image or to different software images.

You can specify these groups manually, using your RME groups and search criteria. You can also use some other selection criterion, such as the current software version or hardware type.

You can run the device upgrades job sequentially or in parallel. After upgrading the devices, you can also specify the reboot order.

To do the Software Distribution, go to **Resource Manager Essentials > Software Mgmt > Software Distribution**.

Logging Into Cisco.com for Software Management Tasks

Login privileges are required for all Software Management tasks that access Cisco.com.

If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the main Cisco web site.

To get access you must have a Cisco.com account. You can register by going to the following URL:
<http://tools.cisco.com/RPF/register/register.do>

To download cryptographic images from Cisco.com, you must have a Cisco.com account with cryptographic access.

To obtain the eligibility to download strong encryption software images:

-
- Step 1** Go to the following URL:
http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y&return_url=http://www.cisco.com
- Step 2** Enter your Cisco.com username and password, and click **Log In**.
 Follow the instructions provided in the page and update the user details.
- Step 3** Click **Accept** to submit the form.
 To verify whether you have obtained the eligibility to download encrypted software:
- Go to the following URL:
http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y&return_url=http://www.cisco.com
 - Enter your username and password, and click **Log In**.
- The following confirmation message is displayed:
 You have been registered for download of Encrypted Software.
-

On CiscoWorks server, you can enter two types of Cisco.com credentials:

- Common Cisco.com credentials for all users of CiscoWorks server.
- Individual user Cisco.com credentials.

To configure common Cisco.com credentials for all users of CiscoWorks server:

-
- Step 1** Select **Common Services > Server > Security > Cisco.com Connection Management > Cisco.com User Account Setup**.
 The Cisco.com User Account Setup dialog box appears.
- Step 2** Enter the following:
- Username—Login ID of the Cisco.com User.
 - Password—Password of the Cisco.com User.
 - Verify Password—Password to confirm.
- Step 3** Click **Apply** to save the user details.
-

You can enter your individual Cisco.com credentials when you perform any Software Management tasks that need access to the Cisco.com server.

If you are accessing Cisco.com over a proxy server, you must enter the proxy server details in the Proxy Server Setup dialog box (**Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**).

For more information on this, see the Online Help or see the *User Guide for Resource Manager Essentials 4.2*.

Setting Up Configuration Management

The Configuration Management application stores the current, and a user-specified number of previous versions, of the configuration files for all supported Cisco devices maintained in the RME. It tracks changes to configuration files and updates the database if a change is made.

You should perform the following tasks:

- Modify Device Configurations and Device Security

You must modify your device configurations to enable Configuration Management to gather the configurations. After your devices become managed, the configuration files are collected and stored in the configuration archive.

- Set up NetConfig

The NetConfig function provides wizard-based templates to simplify and reduce the time it takes to roll out global changes to network devices. These templates can be used to run one or more configuration commands on multiple devices at the same time.

For example, if you want to change passwords on a regular basis to increase security on devices, you can use the appropriate password template to update passwords on all devices at once. A copy of all updated configurations will be stored in the configuration archive.

Setting up Netconfig involves:

- Verifying Device Configuration
- Verifying Device Prompts
- Setting up Transport Protocol Order for Configuration Management

For more information on this, see the Online Help or see the *User Guide for Resource Manager Essentials 4.2*.

Preparing to Use Health and Utilization Monitor

Before using HUM, you need to:

- Create Pollers to monitor the CPU, memory and interface utilization levels. See [Creating a Poller](#).
- Create and set Threshold rules for all the devices selected for polling. See [Creating a Threshold](#).

You can also create Custom Templates for Polling certain performance parameters in a device. See [Creating a Template](#).

For details on the new features introduced in HUM 1.1, see the Whats New section in the *User Guide for Health and Utilization Monitor 1.1*.

Creating a Poller

You can create a Poller by adding devices and selecting appropriate templates to poll the devices. You can also set polling frequencies to poll the devices. The Poller polls the devices for the template MIB variable and collects the device data.

You can use the polled data to analyze the utilization and availability of devices through reports.

To create Pollers, go to **Health and Utilization Monitor > Poller and Template Management > Poller Management**.

For complete details, see the *User Guide for Health and Utilization Monitor 1.1*.

Creating a Threshold

You can set and monitor the optimal value for a MIB variable by defining threshold rules. To do this select a template, choose an appropriate MIB variable, select MIB variable instances and apply a threshold criteria.

You can configure the threshold criteria based on your requirement.

To setup Threshold values go to **Health and Utilization Monitor > Threshold Management > Threshold Setup**.

For complete details, see the *User Guide for Health and Utilization Monitor 1.1*.

Creating a Template

Templates are a logical group of MIB variables that allow you to monitor the performance parameters of a device (such as CPU, memory, interface) for utilization and availability levels.

From the Template Management page you can create a user-defined template, modify the configuration of a user-defined template, export and import a template, delete a user-defined template, and so on.

You can create a user-defined template by grouping new MIB variables. You can also create user-defined templates during Poller creation. To do this use the Add User Defined Template option.

To create a template, go to LMS Portal and select **Health and Utilization Monitor > Poller and Template Management > Template Management**.

For complete details, see the *User Guide for Health and Utilization Monitor 1.1*.

Using CiscoView

CiscoView is a graphical SNMP-based device management tool that provides real-time views of networked Cisco Systems devices.

You can use CiscoView to:

- View a graphical representation of the device, including component (interface, card, power supply, LED) status.
- Configure parameters for devices, cards, and interfaces.
- Monitor real-time statistics for interfaces, resource utilization, and device performance.
- Set user preferences.
- Perform device-specific operations as defined in each device package.
- Manage groups of stackable devices.

For details on the new features introduced in CV 6.1.8, see the *User Guide for Cisco View 6.1.8*.

Using CiscoView Mini-RMON Manager

CiscoView Mini-RMON Manager provides web-enabled real-time remote monitoring (RMON) information to users to facilitate troubleshooting and improve network availability.

If you use CiscoView Mini-RMON Manager with certain Cisco devices, it provides visibility into network issues/problems before they become critical.

See *User Guide for CiscoView 6.1.8* for information about launching and using CiscoView.

Using Device Center

The Device Center provides a device-centric view for CiscoWorks applications and a device-oriented navigation paradigm which provides you device-centric features and information from a single location.

Device Center provides a central point from where you can see a summary and reports for the selected device, invoke various tools on the selected device, and perform the tasks that can be performed on the selected device.

After launching device center, you can perform device-centric activities, such as changing device attributes, updating inventory, Telnet etc. depending on the applications that are installed on the Common Services Server.

You can also launch Element Management tools, reports, and management tasks from the Device Center.

In LMS 3.1, Device Center is enhanced to:

- Display a device in Device Selector although it is not managed by applications that are installed on the local server.
- Display the aggregated summary of a device that is managed in all applications installed on all servers in a DCR domain.

You must set up all the servers in SSO domain to get maximum benefit from this functionality. You can use tools, view reports and perform management tasks according to your privileges.

Using Device Center involves:

- [Launching Device Center](#)
- [Invoking Device Center](#)

Launching Device Center

You can launch Device Center in any of the following ways:

- Launch from the CiscoWorks home page.
Launch the Device Center main page from the CiscoWorks home page and select a device.
To launch device center from CiscoWorks home page, select **Device Diagnostic Tools > Device Center**.
- Launch from CiscoWorks LMS Portal.
Launch the Device Center main page from the LMS Portal home page if you have installed the LMS Portal application on CiscoWorks Server.
- Bookmark the Device Center URL and launch directly from the browser window.
- Launch Device Center for a device from one of the application functions such as Reports.
For example, you can launch Device Center by clicking the Device name from RME Inventory Reports.
- Launch From Third-Party applications by passing the device context as a parameter.

Invoking Device Center

You can invoke Device Center from CiscoWorks home page and perform device-centric activities such as:

- Changing device attributes
- Updating inventory
- Telnet
- Launch Element Management tools
- Generate reports
- Management tasks from the Device Center

To invoke Device Center:

-
- Step 1** Go to the CiscoWorks home page and select **Device Diagnostic Tools > Device Center**.
The Device Center page appears with the Device Selector in the left pane and Device Center overview information in the right pane.
- Step 2** Enter the IP address or device name of the device and click **Go**.
Or
Select a device from the list-tree, in the Device Selector field.
The Device Summary, and Functions Available panes appear.

Step 3 Click any of the links under the Functions Available pane to launch the corresponding application function.

The links are launched in a separate window.

If you enter the device name or IP address of a device not managed by any of the applications installed on the Common Services server, the Functions Available pane displays only the default connectivity tools from Common Services.

For further information on this, see the Using Device Center section in the *User Guide for CiscoWorks Common Services 3.2* or refer the Online Help.

Using Integration Utility

The Integration Utility allows you to launch CiscoView as well as Device Center from an NMS platform even when CiscoView is running on a different system than the NMS. It also allows you to integrate other applications into NMS menu.

See the *User Guide for CiscoWorks Integration Utility 1.7* for information about configuring the Integration Utility.

For details on the NMS supported by the Integration Utility 1.8, see [Supported Network Management Systems](#)

Performing Maintenance on Your CiscoWorks Server

As an administrator, you need to perform maintenance to keep your information updated and to get rid of unnecessary or outdated reports and data on the system.

The CiscoWorks server maintenance tasks include:

- [Performing Regular Backups](#)
- [Purging the Data](#)
- [Maintaining the Log Files](#)

Performing Regular Backups

You can schedule immediate, daily, weekly, or monthly automatic database backups. You should back up the database regularly so that you have a safe copy of the database.

Common Services uses multiple databases to store client application data. These databases are backed up whenever you backup Common Services.

To back up data:

Step 1 Go to the CiscoWorks Home Page and select **Common Services > Server > Admin > Backup**.

The Set Backup Schedule dialog box appears.

Step 2 Enter the following:

- Backup Directory—Location of the backup directory.
- Generations—Maximum number of backups to be stored in the backup directory.
- Time—From the lists, select the time period during which you want the backup to occur. Use a 24-hour format.

The Time field is not enabled if you have selected **Immediate** as the Frequency.

- E-mail—Enter a valid e-mail ID in this field.

You can enter multiple e-mail IDs separated by comma.

The system uses the e-mail ID or e-mail IDs to notify you the following:

- New backup schedules.
- Status of immediate or scheduled backup jobs upon their completion.
- Cancelled backup schedules.

**Warning**

There may be a problem in sending e-mails when you have enabled virus scanner in the CiscoWorks Server.

- Frequency—Select the backup schedule:
 - Immediately—The database is backed up immediately.
 - Daily—The database is backed up every day at the specified time.
 - Weekly—The database is backed up once a week on the specified day and time. Select a day from the Day of week list.
 - Monthly—The database is backed up once a month on the specified day and time. Select a day from the Day of month list.

Step 3 Click **Apply**.

The Schedule Backup message verifies your schedule and provides the location of backup log files.

You can verify backup status by examining the log file at the following location:

On Solaris:

`var/adm/CSCopx/log/dbbackup.log`

On Windows:

`NMSROOT\log\dbbackup.log`

Where *NMSROOT* is the CiscoWorks installed directory.

To restore the backup data, see the Restoring Data Online help or the “Configuring the Server” section of the *User Guide for CiscoWorks Common Services 3.2*.

Purging the Data

Data purging is deleting data that you no longer want. You can purge the data for the following reasons:

- Databases are growing at an uncontrollable rate.
- System performance is affecting the efficiency.
- It is expensive to upgrade hardware.
- To speed up migrations by reducing the volume of data to convert.
- To ensure agility in the disaster recovery plan.

Every LMS application has its own purge policies. You can define these policies by performing these tasks:

Resource Manager Essentials

You can purge RME data by performing these tasks:

- To purge the archived configurations, select **Resource Manager Essentials > Administration > Config Mgmt > Archive Mgmt > Purge Settings**.

The Purge Settings page appears from where you can purge the required configurations.

- To purge the Syslog messages, select **Resource Manager Essentials > Administration > Syslog > Set Purge Policy**.

The Set Purge Policy page appears from where you can purge the required messages.

- To purge the Change Audit data, select **Resource Manager Essentials > Administration > ChangeAudit > Set Purge Policy**.

The Set Purge Policy page appears from where you can purge the required data.

- To schedule purge operations for the RME jobs, select **Resource Manager Essentials > Admin > System Preferences > Job Purge**.

The Job Purge page appears from where you can schedule the required purge activities.

Campus Manager

You can purge Campus Manager data by performing these tasks:

- To delete end hosts and IP phones from User Tracking either on demand or on a specified interval after major acquisition, from the CiscoWorks LMS Home Page select **Campus Manager > User Tracking > Admin > Acquisition > Delete Interval**.

The Delete Interval page appears from where you can delete the required end hosts and IP phones.

- To purge archives or jobs older than a particular date, from the CiscoWorks LMS Home Page select **Campus Manager > User Tracking > Admin > Reports > User Tracking Purge Policy**.

The User Tracking Purge Policy page appears from where you can perform the specified purge activities.

Device Fault Manager

To set up a purge schedule for fault history information, from the CiscoWorks LMS Home Page, select **Device Fault Manager > Configuration > Other Configuration > Daily Purging Schedule**.

The Daily Purging Schedule page appears from where you can set the purge schedule.

Internetwork Performance Monitor

You can purge the database data in IPM with the Purging Report Data option.

To purge report data:

Step 1 Go to the CiscoWorks LMS Home Page select **Internetwork Performance Management > Admin > System Preferences > Purge Settings**.

The Purge Settings page appears.

Step 2 Specify the purge period and click **Apply**.

[Table 5-7](#) lists the purge periods and the settings.

Table 5-7 *Purging Report Data*

Granularity	Purge Settings
Hourly	Runs scheduled purge jobs hourly at the specified time. The default is 32 days.
Daily	Runs scheduled purge jobs daily at the specified time. The default is 180 days.
Weekly	Runs scheduled purge jobs weekly at the specified time. The default is 12 weeks.
Monthly	Runs scheduled purge jobs monthly at the specified time. The default is 12 months.

Health and Utilization Monitor

You can purge HUM data records such as summarization records, Poller failure records, threshold violation records, audit trail records.

HUM stores only the last 24 hours data in the database. Background tasks in HUM summarize this polled data and categorizes the data as 5-minute summarization record, 30-minute summarization record, 3-hour summarization record and 12-hour summarization record.

The summarization of polled data happens every hour. You can purge the summarized data at regular intervals using the Data Purge option.

Data Purge allows you to schedule purging for the following HUM data records:

- 5 Minute Summarization records—Purge all 5-minute summarization data records older than the specified number of days.
- 30 Minute Summarization records—Purge all 30-minute summarization data records older than the specified number of days.
- 3 Hour Summarization records—Purge all 3-hour summarization data records older than the specified number of days.
- 12 Hour Summarization records—Purge all 12-hour summarization data records older than the specified number of days.
- Poller failure records—Purge all failure data records older than the specified number of days.

- Threshold violation records—Purge all threshold violation data records older than the specified number of days.
- Audit trail records—Purge all audit trail data records older than the specified number of days.

By default, all Summarization jobs older than seven days are purged by CiscoWorks HUM.

To schedule Data Purge:

-
- Step 1** Go to LMS Portal and select **Health and Utilization Monitor > Admin > System Preferences**.
- Step 2** Select **Data Purge**.
-

For more details, see the *User Guide for Health and Utilization Monitor*.

Maintaining the Log Files

The Logrot utility helps you manage the log files in a better fashion. Logrot is a log rotation program that can:

- Rotate log when CiscoWorks is running.
- Optionally archive and compress rotated logs.
- Rotate log only when it has reached a particular size.

Logrot helps you add new files easily. Logrot should be installed on the same machine where you have installed Common Services.

You can configure the log files rotation in **Common Services > Server > Admin > Log Rotation**.

For complete details on configuring Logrot, *User Guide for CiscoWorks Common Services 3.2*.

Using CiscoWorks LMS Applications Online Help

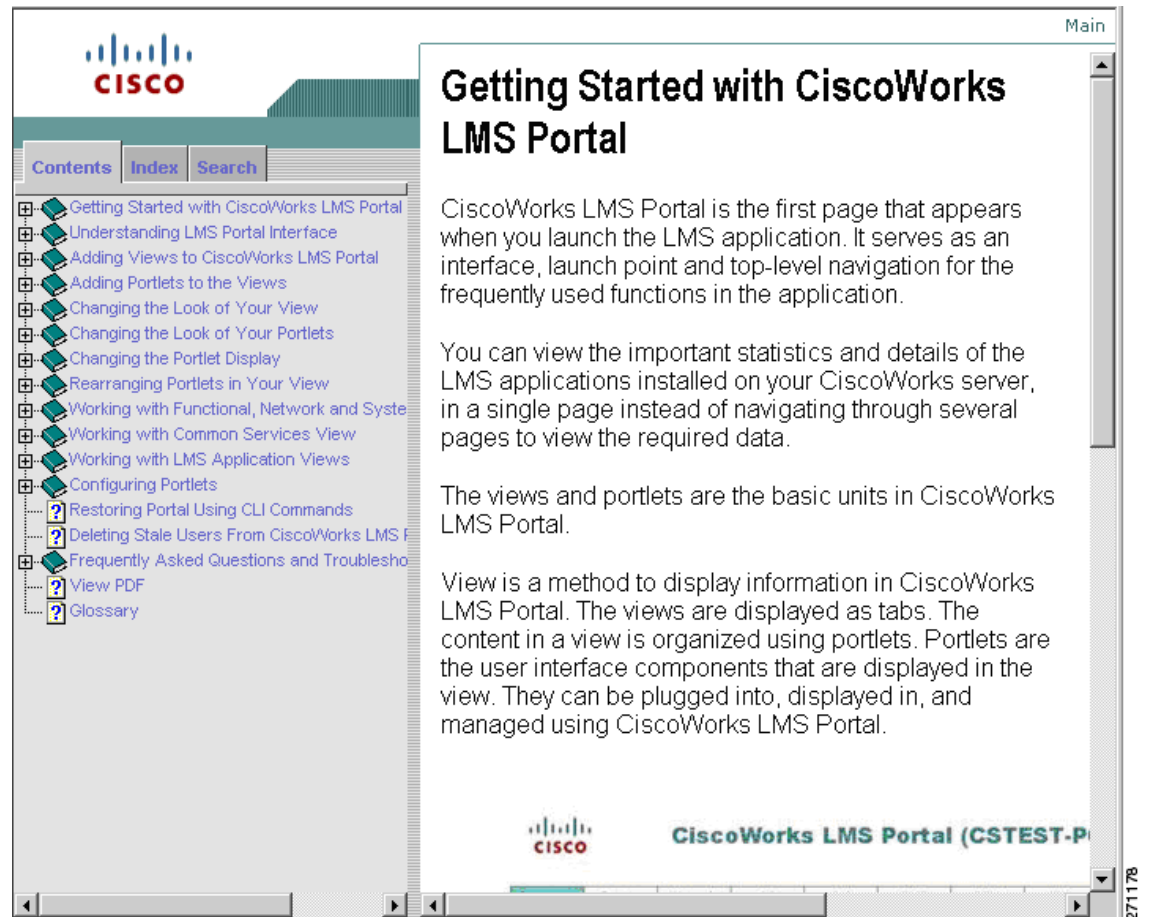
On the CiscoWorks LMS Portal Home Page, click **Help** to Launch the CiscoWorks Online help.

This Help button is at the top right corner of your CiscoWorks LMS Portal Home Page. The CiscoWorks Online help is launched in a separate browser window.

The CiscoWorks Online help window contains the following buttons and links:

Button	Description
Contents (Button)	Displays the Online help table of contents for the launched LMS applications. If you have launched Common Services Online help, the table of contents for the Common Services application appears.
Index (Button)	Displays the index entries for the launched LMS applications. If you have launched Common Services Online help, the index entries for the Common Services application appears.

Button	Description
Search (Button)	<p>Allows you to search for key words within the launched LMS applications.</p> <p>If you have launched Common Services Online help, you can search for any key words within the Common Services Online help.</p> <ul style="list-style-type: none"> • If you want to search for key words in all of the installed LMS applications, you must select All in the application drop-down box (second drop-down box). • If you want to search for key words in a specific LMS application, you must select the application name in the application drop-down box (second drop-down box). <p>That is, if you want to search in RME, select Resource Manager Essentials from the application drop-down box.</p>
Main (Link)	<p>This link is at the top right corner of the CiscoWorks Online help window. See Figure 5-5 for details.</p> <p>Launches the home page of LMS applications Online help.</p> <p>Based on your installed LMS applications, the table of contents area lists the LMS application Online help. See Figure 5-5 for details.</p> <p>If you have installed all the LMS applications, the table of contents lists the following:</p> <ul style="list-style-type: none"> • Campus Manager—Launches the Campus Manager Online help. • CiscoWorks Assistant—Launches the CiscoWorks Assistant Online help. • CiscoWorks Common Services—Launches the Common Services Online help. • Device Fault Manager—Launches the Device Fault Manager Online help. • Device Manager—Launches the CiscoView application (Basic) and CiscoView device packages (ATM Manager, API100, Catalyst 4000 IOS, etc.) Online help. • Internetwork Performance Monitor—Launches the Internetwork Performance Monitor Online help. • LMS Portal—Launches the LMS Portal Online help. • Resource Manager Essentials—Launches the Resource Manager Essentials application (RME User Guide) and device packages (Cisco 10000 Series Routers, Cisco 2600XM Multiservice Router, etc.) Online help. • Health and Utilization Monitor—Launches the Health and Utilization Monitor Online Help. • LMS Glossary (PDF)—Prompts you to open or save the PDF version of LAN Management Solution Glossary that contain the definition for the terms and keywords used in LMS applications.

Figure 5-5 Launching LMS Application Online Help



CHAPTER 6

Troubleshooting and FAQs

This appendix provides troubleshooting information for LMS installation. It contains:

- [Checking Processes After Installation](#)
- [Viewing and Changing Process Status](#)
- [Troubleshooting Your Network Using CiscoWorks Assistant](#)
- [Contacting Cisco Technical Assistance Center \(TAC\)](#)
- [Understanding Installation Error Messages](#)
- [Frequently Asked Questions](#)

Checking Processes After Installation

You can run a self test or view process failures from the CiscoWorks Server.

To run a self test, in the CiscoWorks Homepage select **Common Services > Server > Admin > Selftest**.

To view process failures, in the CiscoWorks Homepage select **Common Services > Server > Reports > Process Status**.

Processes that are not running are displayed in red.

Run the collect server information to check the package errors, if any.

Viewing and Changing Process Status

You can view the status of any process by selecting **Common Services > Server > Admin > Processes** from the CiscoWorks home page.

If you are trying to view and change process status:

- You can start and stop processes from the browser only if you have administrative privileges.
- You can start and stop processes from the CiscoWorks server only if you have local administrative privileges.

To view or change the process status:

-
- Step 1** Go to the CiscoWorks Homepage and select **Common Services > Server > Admin > Processes**.
The Process Management page appears.
- Step 2** Select the processes from this page that you want to stop.
- Step 3** Click **Stop**.
If you select specific processes, the dependent processes also stop.
-

To start processes from the browser:

-
- Step 1** Go to the CiscoWorks Homepage and select **Common Services > Server > Admin > Processes**.
The Process Management page appears.
- Step 2** Select the processes from this page that you want to stop.
- Step 3** Click **Start**.
Only the selected processes are started. The dependent processes are not started.
-

For Windows:

- To stop all processes from the server, enter:
`net stop crmdmgt`
- To start all processes from the server, enter:
`net start crmdmgt`

For Solaris:

- To stop all processes from the server, enter:
`/etc/init.d/dmgt stop`
- To start all processes from the server, enter:
`/etc/init.d/dmgt start`



Caution

Do not start the daemon manager immediately after you stop it. The ports used by daemon manager will be in use for a while even after the daemon manager is stopped. Wait for a few minutes before you restart the daemon manager.

Troubleshooting Your Network Using CiscoWorks Assistant

Cisco Works Assistant helps you collect troubleshooting information from all the servers part of the Multi-server setup and display reports.

For this, you must have configured Single Sign-on and you must also have the same System Identity User configured across all servers as part of the setup.

The two most important troubleshooting functions of CiscoWorks Assistant have been detailed here as follows:

- [Generating Device Troubleshooting Report](#)
- [Generating End Host Down/IP Phone Down Report](#)

Generating Device Troubleshooting Report

CiscoWorks Assistant allows you to generate this report to help you analyze why devices are unreachable. The generated Device Troubleshooting report contains the following details for the selected device:

**Note**

You must install Campus Manager, DFM and RME to view all these details. If these applications are not installed, some of the reports will not be generated.

- Reachability
- Alerts and Syslog Messages
- Differences between two archived running configurations.
- Changes in the device configuration file, inventory, and installed image
- Details of the device topology
- Check Device Attributes (CDA) information
- Details on network inconsistencies, misconfiguration in the physical and logical layout in the discovered network.

**Note**

View Permission Report (Common Services > Server > Reports) to check if you have the required privileges to perform this task.

You can generate this Device Troubleshooting report by selecting **CiscoWorks Assistant > Workflows > Device Troubleshooting**.

For further information on this, refer the Online Help or see the *User Guide for CiscoWorks Assistant 1.1*.

Generating End Host Down/IP Phone Down Report

CiscoWorks Assistant allows you to generate this report to help you locate and track the End Hosts/IP phone in your network, thus providing you the information required to troubleshoot as well as analyze the connectivity issues.

You must install Campus Manager to generate the End Host Down/IP Phone Down report.

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

You can generate the End Host Down/IP Phone Down report by selecting **CiscoWorks Assistant > Workflows > End Host Down/IP Phone Down**.

For further information on this, refer the Online Help or see the *User Guide for CiscoWorks Assistant 1.1*.

Contacting Cisco Technical Assistance Center (TAC)

You can contact the Cisco Technical Assistance Center (TAC) if you had problems while installing Common Services.

Before contacting Cisco TAC, we recommend that you ensure:

- The system hardware and software requirements are met.
- The disk space is not full.
- The CD ROM drive is not defective.

If the above conditions are met, and you still have problems, contact the Cisco Technical Assistance Center.

Cisco TAC representatives may ask you to send them the installation log file in the case of LMS 3.1.

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

Generate a report and email the generated report to Cisco TAC.

To generate the report:

In the CiscoWorks home page, select

Common Services > Server > Admin > CollectServerInformation.

Understanding Installation Error Messages

Table 6-1 shows error messages that might occur during installation and describes the reasons for the errors.

Table 6-1 **Installation Error Messages**

Error Message	Possible Reasons	User Action
CiscoWorks Common Services installation cannot proceed because you are not logged in as an administrator.	You are not logged into Windows with administrator privileges.	Log into Windows with local administrator privileges and try installing again.
The setup program has discovered HP OpenView services running. This will lock some of the CiscoWorks <i>dlls</i> . Stop all HP OpenView services before installing CiscoWorks.	You have installed Device Fault Manager (DFM) on your system. HP Network Node Manager (HPNNM) or NetView is running on the same system.	Stop all HP OpenView services and continue to install CiscoWorks.
Decompression failed on <i>file</i> . The error was for <i>error code per CompressGet</i> .	When you downloaded CiscoWorks Common Services, a transmission error occurred or the installation medium is damaged.	Retry the download. If you still have errors, contact your technical support representative.
General file transmission error. Please check your target location and try again. Error number: <i>error code</i> .	When you downloaded CiscoWorks Common Services, a transmission error might have occurred.	Retry the download. If you still have errors, contact your technical support representative.
Severe: Cannot run the dependency handler.	When you downloaded CiscoWorks Common Services, a transmission error might have occurred. The directory structure of installation is not maintained. This can happen if you download the zip file and extract the contents to install from it.	Retry the download.

Table 6-1 **Installation Error Messages (continued)**

Error Message	Possible Reasons	User Action
Cannot write <i>infoFile</i> or Cannot create <i>infoFile</i> .	A file-write operation failed.	Run the file system checking utility, then repeat the installation. 1. Verify that you have write permission to the destination directory and windows TEMP directory. 2. Repeat the installation. The environment variable <i>%TEMP%</i> provides the location on TEMP directory.
Cannot stop service <i>servicename</i> .	The installation (or reinstallation) tried to stop the service <i>servicename</i> unsuccessfully.	1. Select Control Panel > Services and stop service <i>servicename</i> manually. 2. Proceed with (un)installing.
UseDLL failed for <i>dll</i> .	<i>dll</i> should be available at any time for any process, but Windows did not load it.	<ul style="list-style-type: none"> Check permissions on the system32 directory under <i>%WINDIR%</i>. If the <i>dll</i> is <i>secure.dll</i> or <i>r_inst.dll</i>, check product installation media for errors. Or <ul style="list-style-type: none"> Reinstall Windows.
<i>function</i> failed: DLL function not found.	<i>dll</i> should be available at any time for any process, but Windows did not load it.	<ul style="list-style-type: none"> Check permissions on system32 directory under <i>%WINDIR%</i>. If <i>dll</i> is <i>secure.dll</i> or <i>r_inst.dll</i>, check product installation media for errors. Or <ul style="list-style-type: none"> Reinstall Windows.
OpenFile failed: <i>pathname</i> .	A file open operation failed.	<ul style="list-style-type: none"> Run the file system checking utility, then repeat the installation. Or <ul style="list-style-type: none"> Verify whether you have the read permission on <i>pathname</i>, then repeat the installation.
ProtectFile failed: <i>file</i> : error. WWW admin security may be incomplete.	Setting file permissions failed because you may not be allowed to change them.	Log in as administrator. If you are installing on a FAT file system, CiscoWorks Common Services cannot provide file security.

Table 6-1 **Installation Error Messages (continued)**

Error Message	Possible Reasons	User Action
Launch of isql script failed.	The existing database file is corrupted or the previous version of CiscoWorks Common Services is destroyed. The problem may occur during reinstallation.	Contact your technical support representative.
The product should not be installed in a root directory.	You tried to install the product in a directory of a drive (for example, c:\ or d:\) that is not supported.	Select a directory other than the root directory to install the product.
The product should not be installed in a remote directory.	You tried to install the product in a directory of a drive that is remotely mounted or using the UNC pathname.	Select a directory on a local hard-drive.
The selected directory is not empty. Mixing new and existing files can cause severe problems during installation.	You tried to install in a directory that contains some files.	Remove all files from directory or choose another directory to install the product.
The installer requires temporary workspace. You have less than 8 MB of free space on <i>drive</i> . Free up some space and try again.	There is not enough drive space for temporary installation files.	Make more drive space available (%TEMP%), then rerun installation.
You are attempting to install CiscoWorks Common Services 3.2 on a server that is configured as a Primary Domain Controller or a Backup Domain Controller (PDC/BDC).	You are trying to install the application on a server that is configured as a Primary Domain Controller or a Backup Domain Controller (PDC/BDC).	Install CiscoWorks Common Services 3.2 on another server not configured as PDC / BDC.
You are attempting to install CiscoWorks Common Services 3.2 on an unsupported operating system. The installation will exit when you close this message.	You are trying to install the application on an operating system that does not match System Requirements for the product.	<ul style="list-style-type: none"> Upgrade the Operating System on the Server to a supported version Or <ul style="list-style-type: none"> Install CiscoWorks Common Services 3.2 on another server running a supported Operating System.
You are attempting to install CiscoWorks Common Services 3.2 on <i>operating system</i> and <i>service pack</i> . Please run installation again on a supported platform. Do you want to proceed?	You are trying to install the application on an operating system that does not match System Requirements for the product	Run installation again on a supported platform.

Table 6-1 **Installation Error Messages (continued)**

Error Message	Possible Reasons	User Action
<p>We recommend that you run the installation from a local DVD or a local hard drive to avoid errors that may result from the network being slow or busy.</p> <p>Do you want to proceed?</p> <p>Click Yes to proceed with this installation.</p> <p>Click No to exit installation.</p>	<p>You are trying to install the product from a copy of the DVD or from the DVD drive of another system in the network.</p>	<p>Copy the installable image to a local drive or use local DVD drive.</p>
<p>The installation image is being accessed as \\servername\sharename. Installation can run only from a local or mapped drive.</p> <p>We recommend that you run the installation from a local CD or a local hard drive to avoid errors that may result from the network being slow or busy.</p> <p>Click OK to exit installation.</p>	<p>You are trying to install the product from another system in the network.</p>	<p>Copy the installable image to a local drive or use local CD drive.</p>
<p>The default (or selected) drive <i>drive</i> has a(n) <i>file-system-type</i> file system.</p> <p>This file system does not support file security. The cluster size is <i>cluster size</i> bytes, therefore disk space requirements can be high.</p> <ul style="list-style-type: none"> Choose another directory to install CiscoWorks Common Services Use default or selected directory to install CiscoWorks Common Services 	<p>You are trying to install onto a drive with a non-NTFS (FAT or FAT32) file system.</p> <p>The file system may not support security. The cluster size may be bigger than 4096 bytes.</p>	<p>Click on the directory on which you want to install CiscoWorks.</p>
<p>The product can be installed only in a folder that does not have spaces in its name or can be converted into 8.3 form. Select another destination folder.</p>	<p>The destination directory contains spaces in the directory name and the directory name cannot be converted to a MS-DOS format.</p>	<ul style="list-style-type: none"> Install the product in a directory whose fully qualified pathname does not contain any spaces or has MS-DOS name aliases. <p>Or</p> <ul style="list-style-type: none"> Check the presence of MS-DOS aliases, using dir /x command in a command-line window.

Table 6-1 **Installation Error Messages (continued)**

Error Message	Possible Reasons	User Action
Cannot determine the local Administrators group.	The installation program cannot find one of the built-in Windows user groups. This prohibits CiscoWorks Common Services security setup.	<ol style="list-style-type: none"> 1. Check the Operating System. 2. Reinstall Windows if necessary, 3. Rerun CiscoWorks Common Services installation.
Cannot determine the local Everyone group.	The installation program cannot find one of the built-in Windows user groups. This prohibits the setup of CiscoWorks Common Services security.	<ol style="list-style-type: none"> 1. Check Operating system. 2. Reinstall Windows if necessary, 3. Rerun CiscoWorks Common Services installation.
<p>Installation cannot create the default directory, <i>directory name</i>.</p> <p>You may not have permissions on the default directory or you have specified a read-only device.</p>	You may not have permissions on the directory.	Select another destination directory.
Could not set file permissions.	<p>The installation program cannot set file permissions. Most likely causes are:</p> <ul style="list-style-type: none"> • The account you used to log in to the system has insufficient permissions. • The drive on which you are installing product has a FAT file system. 	<ol style="list-style-type: none"> 1. Correct the problem. 2. Rerun installation program.
<i>task_name</i> is already running! Wait for it to complete and click OK .	One installation subtask is still running.	<ol style="list-style-type: none"> 1. Wait for installation subtask to finish running. 2. Click OK to proceed.
Cannot create/open log file.	The installation program could not create or open the installation log file.	<ol style="list-style-type: none"> 1. Determine why the file could not be created or opened. 2. Correct the problem, then rerun installation. Common causes are lack of disk space or write protection on file. 3. Rerun installation.


Table 6-1 *Installation Error Messages (continued)*

Error Message	Possible Reasons	User Action
<p>Error creating / modifying casuser - <i>name</i>.</p> <p>Click Yes if you want to try again.</p> <p>Click No if you want the Install to terminate.</p>	<p>This error may happen if:</p> <ul style="list-style-type: none"> The passwords that you entered do not match the policies set by System Administrators. <p>Or</p> <ul style="list-style-type: none"> User running the installation does not have permission to create new user on the system. 	<ul style="list-style-type: none"> If you are not authorized to create users on the system, contact your System Administrator. If you are authorized to create users on the system: <ul style="list-style-type: none"> a. Click Yes. A screen appears where you can re-enter the passwords. b. Correct the problem as given in the error message.
Cannot find script to upgrade database.	Problem with database upgrade.	Contact your technical support representative.
Database upgrade failed.	Problem with database upgrade.	Contact your technical support representative.
Database upgrade result unknown.	Problem with database upgrade.	Contact your technical support representative.
The installer has discovered HP OpenView services running. The installation might take significantly longer to complete with these services running.	HP OpenView services are running.	<p>Stop all HP OpenView services before installing CiscoWorks.</p> <p>You do not have to restart the system after stopping HP OpenView.</p>
ODBC Driver Manager 3.510 or later is required by CiscoWorks Common Services. Install ODBC 3.510 first.	CiscoWorks Common Services software requires ODBC Driver Manager version 3.510 or later.	<p>Install Microsoft Data Access Component (MDAC) 2.1 or higher.</p> <p>Make sure that all ODBC Core Components have the same version number.</p> <p>See the Microsoft web site for installation instructions.</p> <p>ODBC is not available from Microsoft as a stand-alone installation but is packaged along with MDAC.</p>
Name lookup failed for <i>hostName</i> . Please configure the hostname and then try installation.	Your hostname is not configured properly.	Configure the hostname and continue installation.

Table 6-1 **Installation Error Messages (continued)**

Error Message	Possible Reasons	User Action
<p>These files are currently being used by another running process. You must stop all processes listed below to proceed successfully with this installation.</p> <p>Click Next to proceed with the installation.</p> <p>Click Cancel to exit.</p>	<p>Some of the executables and DLLs installed by CiscoWorks are locked.</p>	<ol style="list-style-type: none"> 1. Stop all applications. 2. Stop IPM if it is running. 3. Close Browsers and make sure CiscoWorks CLIs are not used at the moment. After stopping all the applications, proceed with the installation. 4. Stop the ACS service if it is installed.
<p>Do you want to verify that CiscoWorks files are no longer being used by running processes?</p> <p>Click Yes to verify that files are no longer in use and that the installation may proceed.</p> <p>Click No to proceed without verification.</p>	<p>Some of the executables and DLLs installed by CiscoWorks are in use.</p>	<p>Verify that files are no longer in use. If some files are in use, stop all processes. To do this:</p> <ol style="list-style-type: none"> 1. Cancel installation. 2. Stop the CiscoWorks and change the startup type from Automatic to Manual. 3. Restart the system. 4. Try to run command net start from MSDOS window. The output should not show any CiscoWorks or CiscoWorks Common Services daemon manager running. 5. Run the installation again.
<p>The instruction at <i>location</i> referenced memory at <i>location</i>. The memory cannot be read.</p> <p>Click OK to terminate the program.</p> <p>Click Cancel to debug the program.</p>	<p>You have installed CiscoWorks Common Services on a Pentium IV machine.</p>	<p>Click OK, and ignore the message. The installation will continue normally.</p>
<p>java.exe has generated errors and will be closed by Windows. You must restart the program. An error log is being created.</p>	<p>This message appears when you install CiscoWorks Common Services on a Pentium IV machine.</p>	<p>Click OK, and ignore the message. The installation will continue normally.</p>

Table 6-1 **Installation Error Messages (continued)**

Error Message	Possible Reasons	User Action
CreateService - <i>service name</i> - The specified service is marked for deletion.	The registry entries related to the service are not deleted during the uninstallation.	<ol style="list-style-type: none"> 1. Restart the machine 2. Reinstall CiscoWorks LAN Management Solution. <p>If the problem still exists:</p> <ol style="list-style-type: none"> 1. Uninstall CiscoWorks LAN Management Solution 2. Restart the machine, 3. Start a fresh installation.
One instance of CiscoWorks Installation is already running. If you are sure that no other instances are running, remove the file C:\CMFLOCK.TXT. The Installation will now terminate.	CiscoWorks installation is already running.	<p>Remove the file C:\CMFLOCK.TXT and retry the installation.</p> <p> Note Parallel installations are not supported. Make sure that no other instance of installation is running, while you start a new installation.</p>
Backup operation failed. Please look at backup directory\backup.log for the reason for failure. Click Retry to take backup again. Click Exit to exit the installation.	The backup process failed.	Retry backing up again.

The LMS Troubleshooting Tips and FAQs is available at this URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/tsd_products_support_troubleshoot_and_alerts.html

The RME Troubleshooting Tips and FAQs is available at this URL:

http://cisco.com/en/US/products/sw/cscowork/ps2073/prod_troubleshooting_guide09186a008036dff2.html

The Campus Manager Troubleshooting Tips and FAQs is available at this URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps563/tsd_products_support_troubleshoot_and_alerts.html

The DFM Troubleshooting Tips and FAQs is available at this URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps2421/tsd_products_support_troubleshoot_and_alerts.html

The IPM Troubleshooting Tips and FAQs is available at this URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps1008/tsd_products_support_troubleshoot_and_alerts.html

The CiscoView Troubleshooting Tips and FAQs is available at this URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps4565/tsd_products_support_troubleshoot_and_alerts.html

Frequently Asked Questions

The following are the list of questions and answers that help you to understand LMS 3.1 better:

Q. On which operating system is LMS 3.1 supported?

A. See [System and Browser Requirements for Server and Client](#) for details.

Q. Which Windows HotFix patches are supported for LMS 3.1?

A. For LMS 3.1, we have tested all the Windows HotFix patches released upto March 2007 that have an impact on LMS:

<http://www.microsoft.com/technet/security/bulletin/ms06-may.msp>

Q. Is LMS 3.1 supported on 64-bit native systems?

A. Yes, LMS 3.1 is supported on native 64-bit systems. See [Operating System Requirements](#) for more information.

Q. Can I install LMS 3.1 with Internet Information Services (IIS) enabled?

A. Yes, you can install. If you click **No** you must stop IIS services before installing LMS 3.1. If you click **Yes** you must change the port from 443 to any other during installation. Also, you must ensure that no other application or process is utilizing this port.

Q. Which TCP and UDP ports does LAN Management Solution 3.1s use?

A. See [LAN Management Solution Port Usage](#) for details.

- Q.** Does LMS 3.1 support virtual machines, such as VMware and VirtualPC?
- A.** Yes, LMS 3.1 supports VMware. See [Server Requirements on Windows Systems](#), for more information.
- Q.** Can I install LMS 3.1 with Windows Domain Controller enabled?
- A.** No, you must disable Windows Domain Controller before installing LMS 3.1.
- Q.** Is LMS 3.1 supported on Solaris x86 (on the x86 CPU)?
- A.** No, LMS 3.1 is not supported on Solaris x86.

- Q.** Is LMS 3.1 supported on multi-homed server?
- A.** Yes, LMS 3.1 is supported on multi-homed server.

A multi-homed machine is a machine that has multiple NIC cards, each configured with different IP addresses. To run CiscoWorks Common Services on a multi-homed machine, there are two requirements:

- All IP addresses must be configured in DNS.
- Owing to restrictions with CORBA, only one IP address can be used by the client or browser to access the server. You must select one IP address as the external address, with which the client will log into the CiscoWorks server.

See the *Release Notes for CiscoWorks Common Services 3.2*:

http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_notes_list.html

- Q.** How do I check the application versions of LMS 3.1?
- A.** You can check the application versions by selecting **Common Services > Software Center > Software Update**. For LMS 3.1 installation, the application versions are:
- CiscoWorks Common Services 3.2
 - Campus Manager 5.1
 - CiscoView 6.1.8
 - Device Fault Manager 3.1
 - Integration Utility 1.8
 - Internetwork Performance Monitor 4.2
 - Resource Manager Essentials 4.2
 - LMS Portal 1.1
 - CiscoWorks Assistant 1.1
 - Health and Utilization Monitor 1.1

If you have installed a licensed version of LMS 3.1, you can check the LMS version in the Products Installed table (**Common Services > Software Center > Software Update**). The LMS version should be 3.1.

- Q.** Can I migrate data from Solaris to Windows and vice versa?
- A.** No, you cannot migrate data between operating systems.

- Q.** Can LMS 3.1 co-exist with other CiscoWorks applications?
- A.** No, LMS 3.1 cannot co-exist with any other CiscoWorks applications.
- Q.** I am currently using a licensed version of LMS 3.1 on Solaris. I want to migrate to Windows. Do I need to get a new license for LMS 3.1 on Windows?
- A.** No, you can use the same LMS 3.1 Solaris license on Windows.
- Q.** When should I install other Network Management Systems (such as HP OpenView Network Node Manager, Netview)?
- A.** You must install other Network Management Systems before installing LAN Management Solution.
- Q.** I have configured CiscoWorks server in ACS mode. Why am I unable to view all of the devices in CiscoWorks server?
- A.** To manage devices in CiscoWorks server, you must configure the devices in Cisco Secure ACS server too. You can view the list of devices that are not configured in the Cisco Secure ACS server using the *Devices that are not configured in ACS Report*.
- You can generate this report by selecting **Common Services > Device and Credentials > Reports**. This report is available only after configuring CiscoWorks with Cisco Secure ACS server.



CHAPTER **A**

User Inputs for Installation

This appendix provides information on the user inputs during LMS 3.1 installation.



Note

For information on the Installation of LMS 3.1, see [Performing New Installation of LMS 3.1](#).

This appendix contains:

- [User Inputs for Typical Installation](#)
- [User Inputs for Custom Installation](#)
- [Password Information](#)

User Inputs for Typical Installation

Enter the following information while installing for the first time in Typical mode:

Table A-1 *User Inputs for New Installation: Typical*

Settings	Value
Components to install	Select the components you want to install.
Password for <i>admin</i> user	No default values. Enter the admin password. For more information on passwords, see Password Information .
Password for System Identity Account	No default values. Enter the System Identity Account password. For more information on passwords, see Password Information .

Enter the following information during an upgrade installation in Typical mode:

Table A-2 *User Inputs for Upgrade Installation: Typical*

Settings	Value
Backup folder	Enter a folder for the backup data. You can also browse and select a folder.
Password for system identity account	No default values. Enter the System Identity Account password. For more information on passwords, see Password Information The installation program retains the System Identity Account password if you are upgrading from LMS 2.5.1 and LMS 2.6.
Components to install	Select the components you want to install. The Select Components dialog box appears if you have installed a previous version of LMS.

Enter the following information while reinstalling in Typical mode:

Table A-3 *User Inputs for Reinstallation: Typical*

Settings	Value
Backup folder	Enter a folder for the backup data. You can also browse and select a folder.
Components to install	Select the components you want to install.

User Inputs for Custom Installation

Enter the following information while installing for the first time in Custom mode:

Table A-4 **User Inputs for a New Installation: Custom**

Settings	Value
Destination folder	The default location is <i>System drive:\Program Files\CSCOpX</i> . Select another location if you want to install in a specific location. We recommend that you specify a short path for the destination folder.
Components to install	Select the components you want to install.
Password for users <i>admin</i> and <i>guest</i> (Mandatory)	No default values. Enter the admin and guest password. For more information on passwords, see Password Information .
Password for System Identity Account (Mandatory)	No default values. Enter the system identity account password. For more information on passwords, see Password Information .
Password for user <i>casuser</i> —This is for Windows only. (Optional)	The password is generated randomly if you leave the field blank.
Password for the CiscoWorks Common Services database. (Mandatory)	Enter the database password. For more information on passwords, see Password Information .
Web server settings: (Mandatory) <ul style="list-style-type: none"> • HTTPS port • Administrator's e-mail address • SMTP server name 	The default values are: <ul style="list-style-type: none"> • Port number 443 • <i>admin@domain.com</i> • <i>localhost name</i>

Table A-4 *User Inputs for a New Installation: Custom (continued)*

Settings	Value
Data for the Self-signed Certificate: (Mandatory)	By default, the self-signed certificate is generated using the organization that Windows is registered to, and the host name. You must enter the host name. You can leave the other fields blank.
<ul style="list-style-type: none"> Country Code State City Organization Name Organization Unit Name Host name E-mail Address 	

Enter the following information during an upgrade installation in Custom mode:

Table A-5 *User Inputs for an Upgrade Installation: Custom*

Settings	Value
Backup folder	Enter a folder for the backup data. You can also browse and select a folder.
Components to install	Select the components you want to install. The Select Components dialog box appears if you have a different set of components in the previous version.
Password for users <i>admin</i> and <i>guest</i> (Optional)	<p>You may change the passwords for the admin and guest users. To keep the existing passwords, leave the fields blank.</p> <p>In the upgrade scenario, you cannot enter the Eval license inputs. Only Purchase license inputs are applicable.</p> <p>For more information on passwords, see Password Information</p>
Password for system identity account (Mandatory)	<p>No default values.</p> <p>Enter the System Identity Account password. For more information on passwords, see Password Information.</p> <p>If you are upgrading from LMS 2.5.1 and LMS 2.6, you can either retain the existing password or enter a new password.</p>
Password for the user casuser (Optional)	<p>If you do not enter a password, the setup program will generate a random password for you. If casuser does not exist, it will be created.</p> <p>However, this is not applicable for Solaris.</p>
Password for the CiscoWorks Common Services Database (Optional)	Leave the fields blank to use the existing password.

Table A-5 *User Inputs for an Upgrade Installation: Custom (continued)*

Settings	Value
Web server settings: <ul style="list-style-type: none"> • HTTPS port • Administrator's e-mail address • SMTP server name (Optional)	You can choose to keep the existing information.
Data for the Self-signed Certificate: (Mandatory) <ul style="list-style-type: none"> • Country Code • State • City • Organization • Organization Unit Name • E-mail Address 	<p>You may change the Self-signed Certificate information. By default, the installation program uses the existing Self-Signed Certificate information.</p> <p>If you want to generate a new certificate, uncheck the Keep Existing Certificate check box, and enter the country code, state, city, company, organization, and host name for HTTPS.</p> <p>You must enter the host name. You can leave the other fields blank.</p>

Enter the following information while reinstalling in Custom mode:

Table A-6 *User Inputs for Reinstallation: Custom*

Settings	Value
Backup folder	Enter a folder for the backup data. You can also browse and select a folder.
Destination folder	The default location is <i>System drive:\Program Files\CSCOpX</i> . We recommend that you specify a short path for the destination folder.
Password for users <i>admin</i> and <i>guest</i> (Optional)	You may change the passwords for the admin and guest users. To keep the existing passwords, leave the fields blank.
Password for system identity account (Mandatory)	You may change the passwords for the system identity account. To keep the existing passwords, leave the fields blank.
Password for user <i>casuser</i> (Optional)	If you do not enter a password, the setup program will generate a random password for you. If <i>casuser</i> does not exist, it will be created.

Table A-6 *User Inputs for Reinstallation: Custom (continued)*

Settings	Value
Password for the CiscoWorks Common Services Database (Optional)	Leave the fields blank to retain the existing password.
Web server settings: <ul style="list-style-type: none"> • HTTPS port • Administrator's e-mail address • SMTP server name (Optional)	You can choose to keep the existing information.
Data for the Self-signed Certificate: (Mandatory) <ul style="list-style-type: none"> • Country Code • State • City • Organization Name • Organization Unit Name • Hostname • E-mail Address 	By default, the self-signed certificate is generated using the organization that Windows is registered to, and the host name. You must enter the host name. You can leave the other fields blank.

Password Information

This appendix provides information on the usage of passwords during installation.

It contains:

- [Password Rules for New Installation](#)
- [Password Rules for Re-installation](#)
- [Password Descriptions](#)

Password Rules for New Installation

The following rules apply for a new installation:

- In Typical mode, admin and System Identity Account passwords are mandatory. Installation program generates guest, casuser, and database passwords randomly.
- In Custom mode, admin, guest, System Identity Account, and database passwords are mandatory. You can either enter the casuser password or allow the installation program to randomly generate it.

Password Rules for Upgrade Installation

The passwords entered during new installation are retained during upgrade installation.

Password Rules for Re-installation

The following rules apply for re-installation:

- In Typical mode, the installation program retains passwords for admin, casuser, guest, and database.
- In Custom mode, you can chose to enter new admin, guest, system identity account, and database passwords or retain the existing passwords. You can either enter the casuser password or allow the installation program to randomly generate it.

Password Descriptions

The types of passwords are as follows:

- [CiscoWorks Admin Password](#)
- [System Identity Account Password](#)
- [CiscoWorks Guest Password](#)
- [LMS Application Database Password](#)
- [Changing CiscoWorks Admin Password](#)
- [Changing casuser Password](#)

CiscoWorks Admin Password

While entering the CiscoWorks Admin passwords, use a minimum of five characters.

System Identity Account Password

While entering the System Identity Account Passwords, use a minimum of five characters.

In a multi-server environment, you must configure all systems part of your multiserver setup with the same System Identity Account password.

See the section Setting up System Identity Account in the *User Guide for CiscoWorks Common Services 3.2* for more details on System Identity Account.

CiscoWorks Guest Password

While entering CiscoWorks Guest passwords, use a minimum of five characters.

LMS Application Database Password

While entering LMS Application Database passwords:

- Use a minimum of five characters and a maximum of 15 characters.
- Do not start the password with a number.
- Do not insert spaces between characters.
- Do not use any special characters.

Changing CiscoWorks Admin Password

You can change your CiscoWorks Admin password by using either the CiscoWorks user password recovery utility or from the GUI, if you want to change it.

- [Changing Admin Password Using Password Recovery Utility](#)
- [Changing Admin Password From GUI](#)

Changing Admin Password Using Password Recovery Utility

To change the CiscoWorks Admin password using the CiscoWorks user password recovery utility:

Step 1 Stop the CiscoWorks Server Daemon Manager by entering the following at the shell prompt:

```
net stop crmdmgt
```

Step 2 Go to *NMSROOT\bin* directory and enter:

```
NMSROOT\bin\resetpasswd username
```

NMSROOT is the directory where you have installed CiscoWorks Common Services.

A message appears:

```
Enter new password for username:
```

- Step 3** Enter the new password for *username*
- Step 4** Start the CiscoWorks Server Daemon Manager by entering at the shell prompt:
- ```
net start crmdmgt
```
- 

## Changing Admin Password From GUI

To change the CiscoWorks admin password from the CiscoWorks server:

- 
- Step 1** Select **Common Services > Server > Security> Single-Server Management > Local User Setup** in the CiscoWorks home page.
- The Local User Setup page appears.
- Step 2** Click **Modify My Profile**.
- The My Profile pop-up window appears.
- Step 3** Enter the password in the Password field.
- Step 4** Re-enter the password in the Verify field.
- Step 5** Enter the e-mail ID in the E-mail field.
- Step 6** Click **OK**.
- 

## Changing casuser Password

You can change the casuser password using **resetCasuser.exe**.

To change the casuser password, do the following:

- 
- Step 1** At the command prompt, enter:
- ```
NMSROOT\setup\support\resetCasuser.exe
```
- Three options are displayed:
1. Randomly generate the password
 2. Enter the password
 3. Exit.
- Step 2** Enter **2**, and press **Enter**.
- A message appears, prompting you to enter the password.
- Step 3** Confirm the password.
- You must know the password policy. If you enter a password that does not match the password policy, the application exits with an error message.
-



CHAPTER **B**

User Tracking Utility

CiscoWorks User Tracking Utility 1.1.1 is a Windows desktop utility that provides quick access to useful information about users or hosts discovered by Campus Manager User Tracking application.

It is a separate utility in the LMS 3.1 DVD that you can install if required.

This section contains:

- [Understanding UTU 1.1.1](#)
- [Hardware and Software Requirements for UTU 1.1.1](#)
- [Downloading UTU 1.1.1](#)
- [Installing UTU 1.1.1](#)
- [Accessing UTU 1.1.1](#)
- [Configuring UTU 1.1.1](#)
- [Searching for Users or Hosts](#)
- [Using Search Patterns](#)
- [Uninstalling UTU 1.1.1](#)
- [Upgrading to UTU 1.1.1](#)
- [Re-installing UTU](#)

Understanding UTU 1.1.1

User Tracking Utility 1.1.1 (UTU 1.1.1) allows users with Help Desk access to search for users or hosts discovered by Campus Manager User Tracking application. UTU comprises a server-side component and a client utility.

To use UTU:

- Campus Manager must be installed and functioning on the Server, and accessible through the network.
- UTU client utility must be installed and running on your local machine.

UTU 1.1.1 has the following additional features:

- Support for silent installation mode for easy deployment.
- Support for communication with Campus Manager server in Secure Sockets Layer (SSL) mode, as well as Non SSL mode.

You can use the UTU search band to search for the Users/Hosts in your network. You can search using user name, host name or IP address, or MAC address. Searching by Host is the default search criteria.

Definitions

Table B-1 explains certain terms and definitions used in User Tracking Utility.

Table B-1 **Definitions**

Term	Definition
Host	Any UNIX or Windows system discovered by User Tracking.
Host Name	Name of the discovered host.
Campus Manager Server	Host name or IP address of CiscoWorks server on which you have installed Campus Manager.
Port	<ul style="list-style-type: none"> Port number to which the host is connected. Port number on which Campus Manager is running on the CiscoWorks server.
Subnet	Subnet to which the host belongs.
User Name	Name of the user who has logged into the host.

Hardware and Software Requirements for UTU 1.1.1

Table B-2 lists the minimum system requirements for UTU.

Table B-2 **System Requirements**

Requirement Type	Minimum Requirements
System Hardware	IBM PC-compatible computer with Intel Pentium processor.
System software	<ul style="list-style-type: none"> Windows 2000 (Professional or Server) with SP4 Windows 2003 Standard Edition Windows 2003 Enterprise Edition Windows XP <p>User Tracking Utility is not supported on Windows Vista Operating System.</p>
Memory (RAM)	128 MB
Additional required software	Campus Manager 5.1
Network Connectivity	Campus Manager 5.1 must be running, and accessible through the network

Downloading UTU 1.1.1

You can download UTU 1.1 and install it from the CiscoWorks User Tracking Utility 1.1.1.exe file.

To download UTU:

-
- Step 1** Locate the file CiscoWorksUserTrackingUtility1.1.1.exe at:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-campus-crypto>
- Step 2** Save the file to a temporary directory on your system.
-

Installing UTU 1.1.1

UTU 1.1.1 supports installation in Normal mode and Silent mode.

To install UTU 1.1.1 in Normal mode:

-
- Step 1** Log into the system with local system administrator privileges.
- Step 2** Navigate to the directory that contains CiscoWorksUserTrackingUtility1.1.1.exe.
- Step 3** Double-click CiscoWorksUserTrackingUtility1.1.1.exe to begin installation.
The User Tracking Utility Welcome screen appears.
- Step 4** Click **Next**.
The Choose Destination Location dialog box appears. By default, UTU is installed in the directory C:\Program Files\CSCOutu.
- Step 5** Click **Next** to install UTU in the default directory.
Or
- a. Click **Browse** to choose a different directory and click **OK**.
 - b. Click **Next** to continue with the installation.
- The Configure CiscoWorks Campus Manager Server Details dialog box appears.
- Step 6** Enter the name or IP address of the server on which Campus Manager is installed.
- Step 7** Enter the HTTP port number of the Campus Manager server.
The default port number is 1741.
- Step 8** Click **Next**.
The following message appears:
- Is CiscoWorks LMS Server SSL Enabled?
- Step 9** Click **Yes** if the Campus Manager server is SSL enabled, otherwise, click **No**.
The Configure LMS Server Authentication dialog box appears. You can also configure these server details after installation.
- Step 10** Enter a valid CiscoWorks Campus Manager Server user name and password.
This is used to verify the validity of the user when searching for users or hosts.

Step 11 Confirm the password and click **Next**.

The Setup Complete dialog box appears.

Step 12 Click **Finish** to complete the installation.

User Tracking Utility 1.1.1 is installed at the destination location you specified in [Step 5](#) above.

However, it does not create a program group under **Start > Programs**. To access the utility, see [Accessing UTU 1.1.1](#).

To install UTU in Silent mode:

At the command prompt, enter:

```
exe-location\CiscoWorksUserTrackingUtility1.1.1.exe -a -s -f1file-location\setup.iss
```

where

- *exe-location* is the directory where you have installed CiscoWorksUserTrackingUtility1.1.1.exe
- *file-location* is the directory where you have installed the setup.iss file.

Do not add a space after the **-f1** option. Use the complete path for *file-location*.

For example:

If the install directory for UTU is C:\utu, enter the following at the command prompt:

```
c:\utu\CiscoWorksUserTrackingUtility1.1.1.exe -a -s -f1c:\utu\setup.iss
```

To configure the server information, modify the setup.iss file before running the silent install. Edit the following fields:

```
[SdShowDlgEdit2-0]
szEdit1= hostname
szEdit2= server-port
Result=1
[AskYesNo-0]
Result=1          <1- SSL Enabled, 0 - SSL Disabled>
[SdShowDlgEdit3-0]
szEdit1=username
szEdit2=password
szEdit3=password
```

You cannot re-install UTU on a system that already has this application installed on it. You must check for existing installations of UTU before beginning a fresh installation.

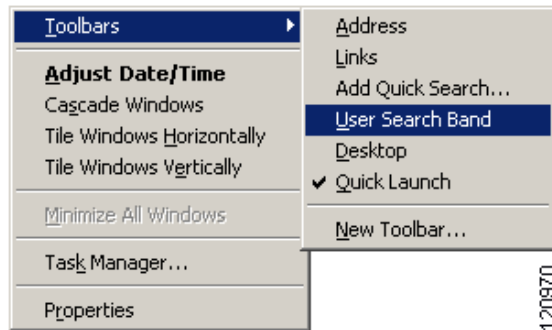
To confirm UTU installation on your system, right-click the taskbar and select **Toolbars** of your machine. You can find User Search Band option in the popup menu.

Accessing UTU 1.1.1

To display the UTU desktop band on the taskbar:

-
- Step 1** Right-click the taskbar of the machine on which you installed UTU.
- Step 2** Select **Toolbars > User Search Band**, as shown in [Figure B-1](#).

Figure B-1 *Selecting the Toolbar*



The UTU desktop band appears on the taskbar with the title User Information.

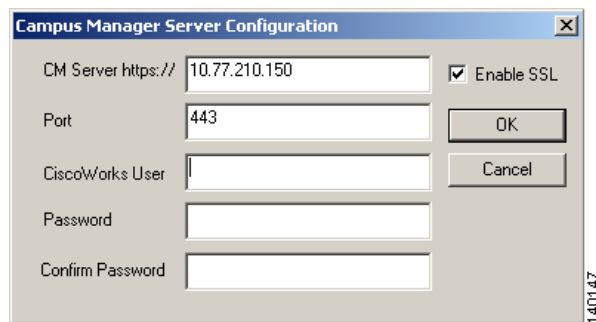
Configuring UTU 1.1.1

You must configure UTU only if you want to change the Campus Manager server configurations that you entered while installing UTU.

To configure UTU:

-
- Step 1** Right-click the User Information search area on the taskbar of the machine on which you installed UTU. A popup menu appears.
- Step 2** Select **Configure**.
The CiscoWorks Campus Manager Server Configuration dialog box appears.
- Step 3** Modify the settings as required.
- Step 4** Click **Enable SSL** to communicate with an SSL enabled server.
The port number changes to 443, which is the default port for SSL. See [Figure B-2](#).

Figure B-2 Enabling SSL



- Step 5** Click **OK** to configure or **Cancel** to quit.
-

Searching for Users or Hosts

You can use UTU search band to search for the users or hosts in your network. You can search using user name, host name or IP address, or MAC address. The default search criterion is host name or IP address of the host.

To search for users or hosts:

-
- Step 1** Enter host name or IP address in the User Information field on the taskbar of the machine.
The default search criterion is host name or IP address of the host. To customize this search criterion:
- Right-click the Users Information search area.
A popup menu appears with the default search criterion **Host/IP** as selected.
 - Select **User**, **Host/IP**, or **MAC Address** from this popup menu.
The selected criterion is set for future searches until you change the criterion.

Table B-3 describes the search criteria in UTU 1.1.1.

Table B-3 Search Criteria in UTU

Search Criterion	Description
User	User name of the hosts in the network.
Host/IP	Host name or IP address.
MAC Address	MAC address of the hosts in the network.

Step 2 Enter any value related to user name, host name, IP address, or the MAC address in the User Information field.

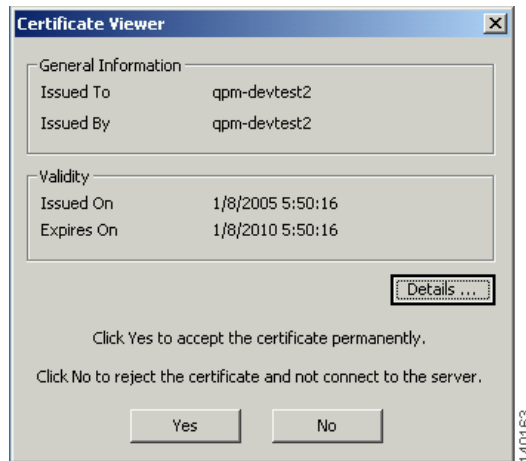
For example, you can enter **10.77.208*** in the User Information field.

Step 3 Press **Enter**.

If your server is not SSL enabled, go to [Step 6](#).

When you query for data from an SSL enabled server, the Certificate Viewer dialog box appears. See [Figure B-3](#).

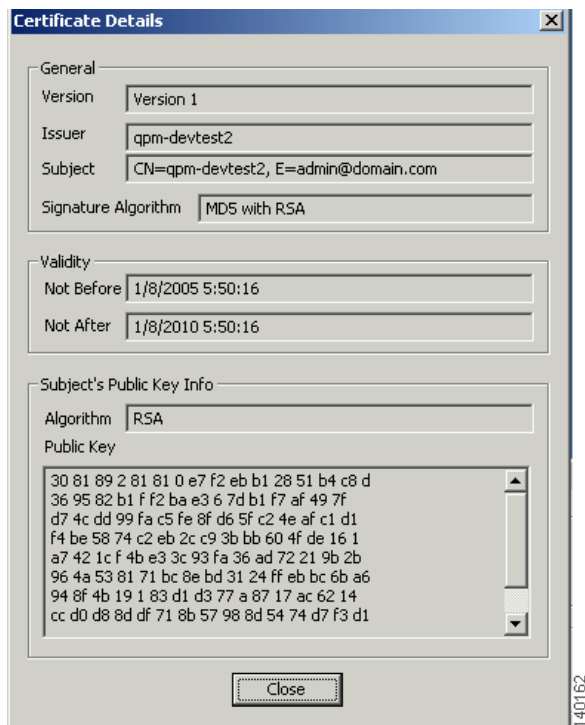
Figure B-3 Certificate Viewer



Step 4 Click **Details** to view the certificate details.

You can verify the authenticity and correctness of the SSL server here. See [Figure B-4](#).

Figure B-4 Certificate Details



Step 5 Click either:

- **Yes** in the Certificate Viewer dialog box to accept and store the certificate. SSL connection is established with the server.

Or

- **No** not to store the certificate and no connection is established with the server.

The Certificate Viewer dialog box appears only while configuring for the first time. If you had clicked **Yes** the first time, you are not prompted to store the certificate during subsequent sessions.

Step 6 Select an entry in the Select Entry popup box.

UTU displays the search results. This is a list of user names, host names, IP addresses, or MAC addresses, in a Select Entry popup menu.

Step 7 Select **Copy All to Clipboard** in the Select Entry popup to copy the complete search result.

Another popup box appears with the details for that particular entry, as described in [Table B-4](#).

Table B-4 Details for Each Entry in Select Entry Box

Entry	Description
User Name	User name of the user logged in to the host.
Host Name	Name of the host discovered by User Tracking.
MAC Address	MAC address of the host.
IP Address	IP address of the host.
Subnet	Subnet to which the host belongs.
Switch	Device name or IP address of the switch.

Table B-4 Details for Each Entry in Select Entry Box (continued)

Entry	Description
Port	Port number to which the host is connected.
Port State	State of the port: Static or Dynamic.
VLAN	VLAN to which the port of the switch belongs.
Port Speed	Bandwidth of the port of the switch.
Port Duplex	Port Duplex configuration details on the device.
Last Seen	Last time User Tracking discovered this host.
Copy to Clipboard	Copies the entries and the details to clipboard.

The search results for the value you enter in the User Information field depends on the default search criterion.

Using Search Patterns

UTU searches for the user or hosts, which match the user name, host name or IP address, or MAC address. You can search for users or hosts by entering a pattern. For example if you enter

- **cisco**, it displays users or hosts, where the user name or host name matches Cisco.
- **cisco***, it displays users or hosts that begin with the word Cisco
- **10.77.208***, it displays host IP addresses that begin with 10.77.208.

Uninstalling UTU 1.1.1

Before you uninstall UTU 1.1.1, you must hide the UTU desktop band.

To do that, right-click the taskbar of the machine on which you installed UTU, and deselect **User Search Band** in the Toolbars popup menu.

To uninstall UTU 1.1.1:

-
- Step 1** Select **Start > Settings > Control Panel > Add/Remove Programs** from the Windows taskbar.
The Add/Remove Programs dialog box appears.
 - Step 2** Select **CiscoWorks User Tracking Utility**.
 - Step 3** Click **Change/Remove**.
The system prompts you to confirm uninstallation.
 - Step 4** Click **Yes**.
 - Step 5** Click **Change/Remove**.
The system prompts you to confirm uninstallation.
 - Step 6** Click **Yes**.
The Remove Programs From Your Computer dialog box appears.

- Step 7** Either:
- a. Click **Yes**
The shared DLL, and UTBand.dll files, are removed.
 - b. Click **OK**.
- Or
- a. Click **No**
The uninstallation proceeds, but it does not completely uninstall UTU. To complete the uninstallation process, you must:
 - b. Go to the command prompt and access the directory where you have installed UTU.
The default directory is C:\Program Files\CSCOutu.
- Step 8** Enter `regsvr32 /u UTBand.dll`
The following message appears:
`DLLUnregisterServer in UTBand.dll failed`
- Step 9** Click **OK**.
- Step 10** Enter `del UTBand.dll`
This removes the UTU installation completely from the machine.
- Step 11** Restart your system.
-

Upgrading to UTU 1.1.1

You can upgrade User Tracking Utility from UTU 1.1 to UTU 1.1.1.

When you install UTU 1.1.1 above UTU 1.1, UTU prompts you to uninstall the previous version. A message appears:

```
WARNING: The setup program has detected a previous version of CiscoWorks User Tracking
Utility. To install CiscoWorks User Tracking Utility 1.1.1, previous version of the
product must be uninstalled. Do you want to uninstall CiscoWorks User Tracking Utility 1.1
now?
Yes/No
```

Click either **Yes** to upgrade, or **No** to quit.

Re-installing UTU

You must not install UTU on a system that already has this application installed on it. You must check for existing installations of UTU before beginning a fresh installation.

To check for an existing installation of UTU:

Step 1 Right-click the taskbar of the machine.

Step 2 Select **Toolbars**.

If you see the User Search Band option, it means you have UTU installed on the system.

You must first uninstall the current installation of UTU, and then start the new installation.



CHAPTER C

Installing the Remote Syslog Collector

This appendix provides general information on how to install the Remote Syslog Collector on a remote Windows or UNIX system to process syslog messages.

The Remote Syslog Collector filters the Syslog messages before forwarding them to the Analyzer process on the RME server.



Warning

Do not install Remote Syslog Collector on a system that has Resource Manager Essentials already installed.

The Remote Syslog Collector and Syslog Analyzer Service on the RME server uses SSL sockets to communicate with each other.

It functions as follows:

1. At startup, the Remote Syslog Collector looks for Syslog Analyzers already subscribed on the RME Server and requests for the latest filter definitions.
- If the Syslog Analyzer is not reachable when queried, the Remote Syslog Collector logs all emblem compliant syslogs in the specified *downtime file* after filtering.

The Syslog Collector Properties file is available at these locations:

- On Solaris:

`NMSROOT/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Collector.properties`

- On Windows:

`NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Collector.properties`

- If the Syslog Analyzer responds with the latest filters, the Remote Syslog Collector applies filters and forwards syslogs to the Syslog Analyzer.
2. At startup, the Syslog Analyzer tries to connect to all the subscribed Remote Syslog Collectors by passing the latest filters.

To subscribe or unsubscribe from a Remote Syslog Collector, select **RME > Tools > Syslog > Syslog Collector Status > Subscribe** using the RME user interface.

After the Remote Syslog Collector connects to the RME Server, the Remote Syslog Collector entry is added to the Collector Status window of the RME Server.

To view the status of the subscribed Syslog Collector, select **Resource Manager Essentials > Tools > Syslog > Syslog Collector Status**.

This section describes how to set up Syslog between RSAC and RME. This involves:

- [Verifying Remote Syslog Collector Server Requirement](#)
- [Installing the Remote Syslog Collector](#)
- [Stopping the Remote Syslog Collector](#)
- [Uninstalling the Remote Syslog Collector](#)

Verifying Remote Syslog Collector Server Requirement

The following section lists the necessary server requirements for Remote Syslog Collector:

- [Table C-1](#) provides the server requirements for Remote Syslog Collector on Solaris.
- [Table C-2](#) provides the server requirements for Remote Syslog Collector on Windows.

Table C-1 Remote Syslog Collector Server Minimum Requirements on Solaris

Requirement Type	Minimum Requirements
Hardware	UltraSPARC CPU
Memory (RAM)	<ul style="list-style-type: none"> • 2 GB RAM and 4 GB swap space on Solaris 9. • 4 GB RAM and 8 GB swap space on Solaris 10.
Operating System	<ul style="list-style-type: none"> • Solaris 9 • Solaris 10
Browser (You need a browser only if you download the RSAC installation files from the RME server.)	<ul style="list-style-type: none"> • Firefox 2.0.

Table C-2 Remote Syslog Collector Server Minimum Requirements on Windows

Requirement Type	Minimum Requirements
Hardware	IBM PC-compatible system with 1 GHz or faster Pentium processor, and 1 GB memory.
Memory (RAM)	2 GB RAM memory requirement with a swap space of 4 GB.
Operating System	<ul style="list-style-type: none"> • Windows Server 2003 Standard and Enterprise Editions with Service Pack 1 and 2 • Windows Server 2003 R2 Standard and Enterprise Editions with Service Pack 1 and 2
Browser (You need a browser only if you download the Remote Syslog Collector installation files from the Essentials server.)	<ul style="list-style-type: none"> • Internet Explorer 6.0 Service Pack 1 • Internet Explorer 7.0 • Firefox 2.0

RSAC 4.2 works only with RME 4.2.

You must uninstall the previous version of RSAC before installing the new RSAC which is provided with LMS 3.1 DVD. To install RSAC 4.1, see [Installing the Remote Syslog Collector](#).

Installing the Remote Syslog Collector

Perform the following to install the Remote Syslog Collector on both platforms.

- [Installing on Solaris](#)
- [Installing on Windows](#)

Prerequisites for installing a Remote Syslog Collector:

- Common Services 3.2 and RSAC 4.2 should be installed.
- If you install Common Services Service Pack on the CiscoWorks server, you must install the same Service Pack on the RSAC server.

The Common Services Service Pack versions must be same in the CiscoWorks Server and RSAC Server.

- RME should not be installed on the server as where you need to install the Remote Syslog Collector. (If RME is installed, the Syslog Collector is installed by default).

Installing on Solaris

To install the Remote Syslog Collector on a Solaris system:

Step 1 Mount the LMS 3.1 DVD.

The RSAC installables are available in the RSAC directory on LMS 3.1 DVD.

Step 2 Enter the following to start the installation:

```
# cd RSAC
# ./setup.sh
```

Step 3 Follow the wizard instructions to install the product.

After the installation of Remote Syslog Collector, select **CiscoWorks Homepage > Software Center > Software Update** to verify the installation. Remote Syslog Collector should be listed.

After Installation, you need to configure the collector.properties file if required. If not, you can use the defaults. See [Understanding the Syslog Collector Properties File](#).

Installing on Windows

To install the Remote Syslog Collector on a Windows system:

-
- Step 1** Navigate to the RSAC folder on the LMS 3.1 DVD.
 - Step 2** Double-click the **Setup.exe** file to start the installation.
 - Step 3** Follow the wizard instructions to install the product.

After the installation of Remote Syslog Collector, select **CiscoWorks Homepage > Software Center > Software Update** to verify the installation. Remote Syslog Collector should be listed.

After Installation, you need to configure the collector.properties file if required. If not, you can use the defaults. See [Understanding the Syslog Collector Properties File](#).

Subscribing to a Remote Syslog Collector

-
- Step 1** Download the Peer certificate from the system where Remote Syslog Collector is running.
 - Step 2** Upload the Peer certificate to the system where Remote Syslog Collector is running.
 - Step 3** Select **Resource Manager Essentials > Tools > Syslog > Syslog Collector Status**.

The Collector Status dialog box appears with this information:

Column	Description
Name	Hostname or the IP address of the host on which the Collector is installed.
Update Time	Date and time of the last update. By default, this dialog box is updated every 5 minutes. Time and time zone are those of the CiscoWorks Server.
Uptime	Time duration for which the Syslog Collector has been up.
Forwarded	Number of forwarded Syslog messages.
Dropped	Number of unprocessed Syslog messages.
Invalid	Number of non emblem compliant Syslog messages.
Filtered	Number of filtered messages. Filters are defined with the Define Message Filter option. For details about defining filters, see the <i>User Guide for Resource Manager Essentials 4.2</i> .
Received	Number of Syslog messages received.

- Step 4** Click **Subscribe**.
The Subscribe Collector dialog box appears.

Step 5 Enter the address of the Common Syslog Collector to which you want to subscribe to.

Step 6 Click **OK**.

The Syslog Analyzer is subscribed the Syslog Collector that you specified. This can be either the Syslog Collector on the RME server, or a remotely installed Syslog Collector.

Starting the Remote Syslog Collector

To start the Remote Syslog Collector, enter `pdexec SyslogCollector` at the command prompt on the machine where Syslog Collector is installed. It starts by default.

Stopping the Remote Syslog Collector

To stop the Remote Syslog Collector, enter `pdterm SyslogCollector` at the command prompt on the machine where Syslog Collector is installed.

Uninstalling the Remote Syslog Collector

Perform the following to uninstall RSAC:

- [Uninstallation on Windows](#)
- [Uninstallation on Solaris](#)

Uninstallation on Windows

To uninstall on a Windows system:

Step 1 Select **Start > Programs > CiscoWorks > Uninstall CiscoWorks**.

The Uninstallation dialog box appears, displaying all of the installed components.

Step 2 Select **Remote Syslog Collector**.

Step 3 Click **Next** to begin uninstalling the selected component.

Uninstallation on Solaris

To uninstall on a Solaris system:

Step 1 Enter these commands as root to start the uninstall program:

```
# cd /  
# NMSROOT/bin/uninstall.sh
```

A message similar to the following appears at command prompt:

```
1) CiscoView 6.1.8  
2) Integration Utility 1.8  
3) CiscoWorks Common Services 3.2  
4) Remote Syslog Collector 4.2  
5) All of the above
```

Select one or more of the items using its number separated by comma or enter q to quit [q]

Step 2 Enter **4** and press **Return**.

Step 3 Follow the prompts from the uninstallation wizard.

Understanding the Syslog Collector Properties File

After installing the Syslog Collector on a remote machine, you need to check the Syslog Collector Properties file to ensure that the Collector is configured properly.

The Syslog Collector Properties file is available at these locations:

- On Solaris:
`NMSROOT/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Collector.properties`
- On Windows:
`NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Collector.properties`

The following table describes the Syslog Collector Properties file:

Timezone-Related Properties	Description
TIMEZONE	<p>The timezone of the machine where the Syslog Collector is running. Enter the correct abbreviation for the timezone. For example, the time zone for India is IST.</p> <p>For the correct Timezone abbreviation, see the Timezone file in the following locations:</p> <ul style="list-style-type: none"> On Solaris: /opt/CSCOpX/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/TimeZone.lst On Windows: NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcsc\data\TimeZone.lst
COUNTRY_CODE	<p>Country code for the Syslog Collector.</p> <p>We recommend that you set the country code variable with the appropriate country code, to make sure that the Syslog timestamp conversion works correctly.</p> <p>For example, if you are in Singapore, you must set the country code variable as COUNTRY=SGP.</p>
TIMEZONE_FILE	<p>The path of the Timezone file. This file contains the offsets for the time zones.</p> <p>After installing the Syslog Collector, ensure that the offset specified in this file is as expected. If it is not present or is incorrect, you can add the Timezone offset according to the convention.</p> <p>The default paths are:</p> <ul style="list-style-type: none"> On Solaris: opt/CSCOpX/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/TimeZone.lst On Windows: NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcsc\data\TimeZone.lst

Timezone-Related Properties	Description
General Properties	
SYSLOG_FILES	<p>Filename and location of the file from which syslog messages are read.</p> <ul style="list-style-type: none"> On Solaris: /var/log/syslog_info On Windows: NMSROOT\log\syslog.log
DEBUG_CATEGORY_NAME	<p>Name Syslog Collector uses for printed ERROR or DEBUG messages.</p> <p>The default category name is SyslogCollector.</p> <p>We recommend that you do not change the default value.</p>
DEBUG_FILE	<p>Filename and location of the Syslog Collector log file containing debug information:</p> <ul style="list-style-type: none"> On Solaris: /var/adm/CSCOpX/log/CollectorDebug.log On Windows: NMSROOT\log\CollectorDebug.log
DEBUG_LEVEL	<p>Debug levels in which you run the Syslog Collector.</p> <p>We recommend that you retain the default INFO, which reports informational messages. Setting it to any other value might result in a large number of debug messages being reported.</p> <p>If you change the debug level, you must restart the Syslog Collector.</p> <p>The values for the Debug levels are:</p> <ul style="list-style-type: none"> Warning Debug Error Information
DEBUG_MAX_FILE_SIZE	<p>The maximum size of the log file containing the debug information.</p> <p>The default is set to 5 MB.</p> <p>If the file size exceeds the limit that you have set, Syslog Collector writes to another file, based on the number of backup files that you have specified for the DEBUG_MAX_BACKUPS property.</p> <p>For example, if you have specified the number of backups as 2, besides the current log file, there will be two backup files, each 5MB in size. When the current file exceeds the 5 MB limit, Syslog Collector overwrites the oldest of the two backup files.</p>
DEBUG_MAX_BACKUPS	<p>The number of backup files that you require. The size of these will be the value that you have specified for the DEBUG_MAX_FILE_SIZE property.</p>

Timezone-Related Properties	Description
Miscellaneous Properties	
READ_INTERVAL_IN_SECS	The interval at which the Collector polls the syslog file. The default is set to 1 second.
QUEUE_CAPACITY	The size of the internal buffer, for queuing syslog messages. The default is set to 100000.
PARSER_FILE	The file that contains the list of parsers used while parsing syslog messages. <ul style="list-style-type: none"> On Solaris: opt/CSCOpX/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/FormatParsers.lst On Windows: NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcsc\data\FormatParsers.lst
SUBSCRIPTION_DATA_FILE	The Syslog Collector data file that contains the information about the Syslog Analyzers that are subscribed to the Collector. <ul style="list-style-type: none"> On Solaris: opt/CSCOpX/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Subscribers.dat On Windows: NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Subscribers.dat
FILTER_THREADS	The number of threads that operate at a time for filtering syslog messages. The default is set to 1.
COLLECTOR_PORT	The default port of the Syslog Collector. The default is set to 4444. The port where the collector listens for registration requests from Syslog Analyzers.



INDEX

A

accessing CiscoWorks server [5-2](#)
Application [3-7](#)
Application scaling numbers
 solution server [3-7](#)
 standalone server [3-7](#)
audience for this document [xvii](#)

C

cautions, significance of [xviii](#)
cautions regarding
 daemon manager, starting and stopping [6-2](#)
 link to installation directory, removing [4-9](#)
CiscoWorks [A-8](#)
CiscoWorks applications, preparing to use [5-48](#)
 Campus Manager [5-48](#)
 CiscoView [5-65](#)
 Device Center [5-65](#)
 DFM [5-52](#)
 Integration Utility [5-67](#)
 IPM [5-55](#)
 application settings [5-55](#)
 operations, managing [5-56](#)
 working with collectors [5-57](#)
 RME [5-58](#)
CiscoWorks Common Services Overview [1-1](#)
CiscoWorks LMS Portal, understanding [5-3](#)
CiscoWorks LMS Portal home page [5-3](#)
CiscoWorks Online help, using [5-71](#)
CiscoWorks processes [4-47](#)
CiscoWorks Server

 before you begin setup [5-15](#)
CiscoWorks Server, managing devices [5-46](#)
CiscoWorks Server, performing maintenance [5-67](#)
 data purge [5-69](#)
 log files, maintaining [5-71](#)
CiscoWorks Server, performing regular backups [5-67](#)
CiscoWorks Server, setting up [5-15](#)
 AAA modes, understanding [5-21](#)
 about CiscoWorks Assistant [5-22](#)
 DCR, understanding [5-16](#)
 DCR modes [5-16](#)
 Master DCR [5-17](#)
 Slave DCR [5-17](#)
 Standalone DCR [5-18](#)
 deployment methods [5-22](#)
 device management, understanding [5-16](#)
 device management modes [5-18](#)
 multi-server setup, understanding [5-15](#)
 single-server setup, understanding [5-15](#)
 single sign-on, understanding [5-21](#)
CiscoWorks Server-ACS integration [5-40](#)
composition of LMS [1-2](#)
Concurrent users [3-8](#)
configuring DFM (minimum setup)
 SNMP trap receiving and forwarding, configuring
 trap forwarding, configuring [5-53](#)
 trap receiving port, updating [5-52, 5-54](#)
 traps, enabling devices to send [5-52](#)

D

database password rules [A-8](#)
device credentials, LMSApplications [2-16](#)

device support [1-13](#)
 disabling FIPS [2-9](#)
 documentation
 audience for this [xvii](#)
 typographical conventions in [xvii](#)

E

enabling FIPS [2-9](#)
 Evaluation mode [3-10](#)

F

FIPS, enabling/disabling [2-9](#)

G

getting started with LMS [5-1](#)
 Guest password rules [A-8](#)

I

installation [4-1, 6-1](#)
 before installation [3-1](#)
 before you begin [3-3](#)
 general installation notes [3-3](#)
 Solaris installation notes [3-4](#)
 Windows installation notes [3-5](#)
 new installations
 password rules for [A-8](#)
 reinstallations
 password rules for [A-7](#)
 task overview [3-1, 4-46](#)
 upgrades
 password rules for [A-7](#)
 user inputs for
 custom installations [A-3](#)
 typical installations [A-2](#)

installation, preparing to [3-1](#)
 installation tasks overview [4-46](#)
 installation terms overview [3-1](#)
 Cisco.com user ID and password [3-2](#)
 CiscoWorks Admin Password [3-2](#)
 CiscoWorks Guest password [3-2](#)
 LMS application database password [3-1](#)
 Self signed certificate [3-2](#)
 SMTP Server [3-2](#)
 System Identity Account password [3-2](#)

installing NSPECHO

 system software, verifying [5-67](#)

installing RSAC (see RSAC) [C-13](#)

integrating CiscoWorks Server with ACS [5-40](#)

 AAA mode setup [5-43](#)

 ACS server setup [5-42](#)

 ACS support [5-40](#)

 assigning roles to users [5-45](#)

 before you begin [5-42](#)

 CiscoWorks authentication roles [5-41](#)

 impact of installing CiscoWorks applications [5-45](#)

 verifying LMS applications [5-46](#)

Integration Utility

 supported NMS [1-12](#)

K

key features of LMS 3.0 [1-4](#)

L

license file [3-8](#)

license file, installing [3-11](#)

license information [3-5](#)

Licensing LMS [3-8](#)

 Eval license [3-10](#)

 license file [3-8](#)

 NFR license [3-10](#)

PAK [3-8](#)

LMS

accessing CiscoWorks Server [5-2](#)

Application scaling numbers [3-7](#)

before starting to use [5-2](#)

before uninstalling [4-49](#)

Composition of [1-2](#)

Concurrent users [3-8](#)

getting started with [5-1](#)

key features [1-4](#)

POE support [1-5](#)

third party tools and software changes [1-5](#)

license information [3-5](#)

Licensing Your Product [3-8](#)

logging into CiscoWorks Server [5-3](#)

prerequisites [2-1](#)

System and Client requirements [2-1](#)

uninstalling [4-49](#)

LMS, administering [5-9](#)

LMS Setup Center [5-9](#)

System setup and administrative tasks [5-10](#)

LMS 3.0 new installation [4-2](#)

silent mode [4-23](#)

Solaris [4-2](#)

custom [4-9](#)

typical [4-6](#)

verifying installation [4-47](#)

Windows [4-14](#)

custom [4-20](#)

typical [4-17](#)

LMS Administration parameters, configuring [5-9](#)

LMS applications, launching [5-8](#)

LMS Portal views [5-6](#)

LMS Port Usage [2-13](#)

LMS reinstallation [4-52](#)

LMS uninstallation

Solaris [4-50](#)

Windows [4-51](#)

logging into CiscoWorks Server [5-3](#)

M

messages you may see during installation [6-5](#)

N

NFR license [3-10](#)

NSPECHO

installing

system software, verifying [5-67](#)

O

Online help, using [5-71](#)

P

PAK [3-8](#)

password information

Admin password rules [A-8](#)

Guest password rules [A-8](#)

new installation rules [A-8](#)

upgrade and reinstallation rules [A-7](#)

portlets [5-7](#)

ports

forwarding [5-54](#)

listening [5-54](#)

Port usage [2-13](#)

prerequisites [2-1](#)

prerequisites for installation

terminal server support [2-9](#)

about Terminal Services [2-9](#)

R

required device credentials for LMS [2-16](#)

RSAC (Remote Syslog Analyzer Collector)

Common Syslog Collector, subscribing to [C-16](#)

installing [C-13](#)

- Remote Syslog Collector [C-15](#)
- Syslog Analyzer Collector [C-15](#)
- uninstalling RSAC [C-17](#)

properties file [C-18](#)

- COLLECTOR_PORT [C-21](#)
- COUNTRY_CODE [C-19](#)
- DEBUG_CATEGORY_NAME [C-20](#)
- DEBUG_FILES [C-20](#)
- DEBUG_LEVEL [C-20](#)
- DEBUG_MAX_BACKUPS [C-20](#)
- DEBUG_MAX_FILE_SIZE [C-20](#)
- FILTER_THREADS [C-21](#)
- PARSER_FILE [C-21](#)
- QUEUE_CAPACITY [C-21](#)
- READ_INTERVAL_IN_SECS [C-21](#)
- SUBSCRIPTION_DATA_FILES [C-21](#)
- SYSLOG_FILES [C-20](#)
- TIMEZONE [C-19](#)
- TIMEZONE_FILE [C-19](#)

server requirements, verifying [C-14](#)

stopping [C-17](#)

uninstalling [C-17](#)

upgrading [C-15](#)

S

scaling numbers of LMS 3.0 [3-7](#)

Single server setup [5-24](#)

- default credentials, setting up [5-26](#)
- device management mode, setting up [5-25](#)
- devices, adding [5-27](#)
 - methods [5-27](#)
- devices, managing [5-32](#)
- LMS server, managing [5-24](#)
- multiple ciscoworks servers, setting up [5-35](#)
 - before setting up [5-36](#)
 - multi-server setup tasks [5-37](#)
 - terms you should know [5-35](#)

SNMP trap receiving and forwarding, configuring

- trap receiving port, updating [5-52, 5-54](#)
- traps, enabling devices to send [5-52](#)
- traps forwarding, configuring [5-53](#)

Solaris patches [2-10](#)

stopping RSAC [C-17](#)

supported devices [1-13](#)

Supported Network Management Systems [1-12](#)

system requirements

- client system [2-8](#)
- Solaris Server [2-4](#)
- Windows Server [2-6](#)

T

terminal server support [2-9](#)

- about Terminal Services [2-9](#)
- enabling or disabling Terminal Services
 - on Windows 2003 [2-9](#)

Troubleshooting [6-3](#)

troubleshooting installation

- CiscoWorks administration password, changing [6-10](#)
- messages, understanding [6-5](#)
- processes, checking [6-3](#)
- process status, viewing and changing [6-1](#)

typographical conventions in this document [xvii](#)

U

uninstalling

- RSAC [C-17](#)

upgrading LMS

- local upgrade on Solaris [4-26](#)
 - custom [4-32](#)
 - typical [4-28](#)
- local upgrade on Windows [4-37](#)
 - custom [4-42](#)
 - typical [4-39](#)

remote upgrade on Solaris [4-36](#)

remote upgrade on Windows [4-46](#)

upgrading RSAC [C-15](#)

User Tracking Utility

installing [B-3](#)

hardware requirements [B-2](#)

software requirements [B-2](#)

uninstalling [B-9](#)

key terms in [B-2](#)

using

pattern use in searching [B-9](#)

V

Views [5-6](#)

