Release Notes for CiscoWorks LAN Management Solution 4.0

Revised: September, 2010, OL-20726-02

Contents

This Release Notes is for CiscoWorks LMS 4.0 on Solaris and Windows platforms.

This document has the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

CiscoWorks LAN Management Solution (LMS) provides powerful features that enable you to configure, monitor, troubleshoot, and administer Cisco networks. It also supports new Cisco technologies such as Identity, EnergyWise, Auto Smartports, and Smart Install.

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

CiscoWorks LMS 4.0 categorizes options to the following underlying core functions in this release:

- Monitoring
- Inventory Management
- Configuration
- Reporting
- Administration
- Work Center Management

This document provides instructions for downloading and installing CiscoWorks LAN Management Solution (LMS) 4.0 on Windows and Solaris Operating Systems. It also provides information on the new features supported in LMS 4.0 and points you to the known problems in LMS 4.0.

What's New in This Release

The following are the new features in LMS 4.0:

- Getting Started Workflow
- Navigating Menus
- Work Centers
- Dashboards
- Search and Fault Bar
- Template Center
- CiscoWorks Local Role-based Access Control
- Unified Grouping Services
- Unified Device Manager
- EnergyWise
- Identity
- Auto Smartports
- Smart Install
- Fault Monitor
- Event Monitor
- Troubleshooting Workflow
- Report Center

- VRF-lite support for Catalyst 3000 and Catalyst 4000 devices
- Third-Party Software and Tool Changes

> **Note** The supported screen resolution for LMS 4.0 is 1024x768 pixels. We recommend you do not use browser zoom in and zoom out features in LMS 4.0.

Getting Started Workflow

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

When you login to CiscoWorks LMS Server as a user with Super Admin and Network Administrator roles, the Getting Started page appears. The Introduction page of the Getting Started workflow appears. The Introduction page lists the new features in CiscoWorks LMS 4.0.

When you login as a user with roles other than Super Admin and Network Administrator, the Default Dashboard appears.

You can do the following tasks using the Getting Started workflow:

- Configuring multiserver Setup
- Configuring e-mail, cisco.com and proxy settings
- Updating software and device packages
- Migrating data
- Configuring RCP and SCP Credentials, security, backup and authentication settings
- Managing devices and credentials
- Managing user roles and users
- Links to advanced functionalities and settings

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

Navigating Menus

The LMS 4.0 menus are organized as follows:

Menu	Description
My Menu	My Menu helps you to consolidate information specific to particular functions as dashboards. My Menu also enables you to group data from different functions into a single page. You can add, view and manage dashboards using the following options in My Menu: • My Dashboard • Public Dashboards • Default Dashboards
Monitor	You can use the Monitor menu for monitoring and troubleshooting your network in LMS. The menu also offers performance and fault management tasks and diagnostic tools.
Inventory	You can use the Inventory menu for discovering network devices, managing device credentials, generating inventory and device reports, and managing inventory dashboards.
Configuration	You can use the Configuration menu for deploying configurations on devices, updating software images, archiving and comparing device configurations, configuring VLANs, configuring technologies, converting standalone switches to a virtual switching system. Configuration menu also offers compliance tasks and you can generate configuration compliance reports.
Reports	You can use the Reports menu to view and generate reports such as device reports, fault and event reports, audit reports, inventory reports, performance reports, cisco.com reports, and system reports.
Admin	You can use the Admin menu for performing all the network and system administration activities such as Device Credential Repository settings, collection settings, tools settings, purge settings, report settings, group management, server administration, software center.
Work Centers	You can use the WorkCenter menu for configuring Cisco technologies such as Identity, EnergyWise, Smart Install, and Auto Smartports on devices using LMS.
Legacy	You can use the Legacy menu to perform LMS functions by using the legacy LMS 3.x navigation menus.

Work Centers

CiscoWorks LMS 4.0 provides complete lifecycle management of:

- Cisco solutions such as:
  - Identity
  - EnergyWise
- Network features such as:
  - Auto Smartports
  - Smart Install

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

Dashboards

Dashboards provide you with a quick snapshot of specific information on Fault, Configuration, Accounting, Performance, Security (FCAPS) functionality. The following functional dashboards are available in LMS:

- Monitoring Dashboard
- Identity Dashboard
- EnergyWise Dashboard
- Inventory Dashboard
- Configuration Dashboard
- Device Status Dashboard
- System Dashboard

Search and Fault Bar

This section explains:

- Search Bar
- Fault Bar

Search Bar

CiscoWorks LMS comes with a new search bar that can be accessed from across all pages. Using the new improved search, you can perform keyword and object-based search on the following topics:

- Devices
- End Hosts
- Tasks
- Jobs
- Help

Fault Bar

CiscoWorks LMS has a new fault bar that floats across all pages. Using the fault bar, you can view the real-time summary of Critical, Warning and Info faults.

Template Center

The Template Center in LMS 4.0 provides you with a list of system-defined templates. These templates contain configuration commands that can be deployed on the devices in your network. These templates are deployed using Deploy Template jobs in LMS.

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

You can perform the following tasks:

- Deploying templates
- Managing templates
- Importing templates
- Assigning templates to users

CiscoWorks Local Role-based Access Control

From LMS 4.0, CiscoWorks Local Role-based Access Control is available for authorization. After authentication, your authorization is based on the privileges that have been assigned to you.

Using this mode of authentication you can:

- Create user-defined roles
- Customize existing roles
- Import and export roles and users
- Assign one or more roles to LMS users
- Set a default role.

You can enable:

- Full authorization
- Task authorization
- Device group authorization

Unified Grouping Services

LMS 4.0 combines the device grouping with a new attribute list. LMS 4.0 supports 200 device groups.

The other grouping services that are available in LMS are:

- Fault Group - supports 50 groups
- IPSLA Collector Group - supports 100 groups
- Port and Module Group - supports 100 groups

Unified Device Manager

In LMS 4.0, Unified Device Manager (UDM) provides centralized device management using a centralized policy configuration. UDM identifies managed devices after verifying the configured policy and the license count.

The different device states in LMS 4.0 are:

- Managed state
- Suspended state
- Unmanaged state
- Managed Devices not matching the Policy state

EnergyWise

Cisco EnergyWise is a comprehensive program for power management in your network. Cisco EnergyWise enables companies to measure, manage, and reduce the power consumption of network infrastructure and network-attached devices, and to increase cost savings.

Using EnergyWise in LMS 4.0 you can:

- Assess the EnergyWise readiness of your network
- Discover and enable EnergyWise on devices
- Configure and implement energy management policies
- Monitor power consumption using EnergyWise dashboard
- Generate and view energy and cost savings graphs reports

EnergyWise Reports quantify the energy used and saved by the network.

The types of EnergyWise reports are:

- EnergyWise Device Power Usage Quick Report
- EnergyWise Port Power Usage Report
- EnergyWise Power Usage Report
- EnergyWise Cost Saving Report

For more information on EnergyWise refer to *Technology Work Centers in CiscoWorks LAN Management Solution 4.0.*

Identity

Cisco TrustSec Identity, earlier known as Cisco Identity-based Networking Services (IBNS), a part of the Cisco Trust and Identity Management Solution, is an integrated solution that comprises of several Cisco products, and offers authentication, access control, and user policies to secure network resources and connectivity.

Using Identity in LMS 4.0 you can:

- Assess the Identity readiness of your network
- Discover and enable Identity on devices
- Enable phased deployment of Cisco TrustSec Identity using various security modes with minimal impact to your network
- Strengthen the security of your network
- Provide differentiated services to your end users
- Assign resources dynamically to the correct VLAN
- Automate security policy enforcement
- Monitor authentication and authorization trends through charts and graphs

Identity reports display information on the various users of the CiscoWorks LMS 4.0 network.

The types of Identity Reports are:

- Authenticated Users Report
- Authentication Failure Report
- Authorization Failure Report
- User-specific Report

For more information on Identity refer to *Technology Work Centers in CiscoWorks LAN Management Solution 4.0.*

Auto Smartports

Auto Smartports macros dynamically configure ports based on the device type detected on the port. When the switch detects a new device on a port it applies the appropriate Auto Smartports macro on the port.

Using Auto Smartports in LMS 4.0 you can:

- Assess the readiness of your network for Auto Smartports
- Discover Auto Smartports-capable devices, and enable Auto Smartports on them
- Dynamically configure Auto Smartports macros on ports, based on the device type detected on the port
- Dynamically enable quality of service (QoS), security features, and a dedicated VLAN using Auto Smartports macros
- Monitor Auto Smartports through the Auto Smartports report

For more information on Auto Smartports refer to *Technology Work Centers in CiscoWorks LAN Management Solution 4.0.*

Smart Install

Smart Install is a plug-and-play configuration and image-management feature that provides zero-touch deployment for new switches. Smart Install enables you to ship a switch to a location, place it in the network and power it on with no configuration required on the switch.

Using Smart Install in LMS 4.0 you can:

- Assess the readiness of your network for Smart Install capable switches and directors
- Discover and enable Smart Install on Smart Install-capable devices
- Manage configuration files and images of clients in the Smart Install director
- Configure DHCP settings for Smart Install
- Monitor Smart Install through the Smart Install report

For more information on Smart Install refer to *Technology Work Centers in CiscoWorks LAN Management Solution 4.0.*

Fault Monitor

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

Fault Monitor collects information on faults and events from all devices in real-time and displays the information for a selected group of devices. Fault Monitor allows you to own the faults or clear them. We can annotate faults or we can send notifications as well.

Event Monitor

Event Monitor is a centralized page where you can view the event details of all devices in the network. Event Monitor displays the fault history, syslog, and system events that were generated by the network in the:

- Last one hour
- Last two hours
- Last four hours
- Last eight hours
- Last one day

Troubleshooting Workflow

Troubleshooting workflow in LMS collects information across devices in the network and helps you to overcome network management challenges.

You can troubleshoot the following problems using this workflow:

- Network connectivity problems
- Device diagnostics

Report Center

Reports Center provides a single launch point where all reports can be generated, and viewed from a common report management area.

Using Report Center in LMS 4.0 you can:

- Generate reports which are grouped as:
  - Inventory
  - Performance
  - Switch Port
  - Cisco.com
  - Technology
  - System
  - Fault and Event
  - Audit
- View Report Archives

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

- Configure system preferences for managing reports
- Report Designer

  You can create new report templates customized for your requirements.

VRF-lite support for Catalyst 3000 and Catalyst 4000 devices

LMS 4.0 supports VRF-lite technology in catalyst 3000 and catalyst 4000 devices.

Third-Party Software and Tool Changes

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

- Support for Windows 2008 Standard Edition and Enterprise Edition
- WinPcap upgrade to 4.0.2
- Daylight Savings Timezone tool upgrade to 1.3.11
- Firefox 3.6.x support on client systems
- Java Plug-in upgrade to 1.6.0_19
- Apache upgrade to 2.2.10
- Java Runtime Environment (JRE) 1.6.0_19

Time Zone and Offset Settings

LMS supports many time zones. However, applications that have scheduling and reporting functions, and applications that produce or use time stamps vary based on:

- Server and client—Time stamps can differ between server and client if they are located in different time zones.

- Platforms—Windows and UNIX servers support different time zones and are not synchronized.

Table 1 shows time zone acronyms supported in the CiscoWorks applications that use the time zone feature.

- Column 1—Alphabetically lists the supported CiscoWorks time zone acronyms. Change Audit reports may display time zone information differently.

- Column 2—Lists the spelled out time zone definition.

- Column 3—Lists the area covered by the time zone.

- Column 4—Lists the column's offsets from Greenwich Mean Time (GMT).

- Column 5—Lists the time zone setting for that zone's server.

- Column 6—Lists the resulting output in reports.

If you generate reports, the output will vary depending on whether the data has been processed through Perl or Java. Table 1 also provides possible outputs for either case scenario.

To ensure that time zones are translated correctly—especially when your devices, servers, and clients are in different time zones—follow these guidelines:

- While configuring time zones on managed devices, use the acronyms listed in the *Time Zone Acronym Setting on Device* column. To set time zones on devices, use the command described in the device-specific Command Reference documentation.

- The device should be configured to send Syslogs with the appropriate time zone acronym that indicates whether daylight savings is in effect at the time of sending the Syslog. This is to ensure that the Syslog analyzer or Essentials uses the correct acronym for time conversion.

- While configuring time zones on CiscoWorks servers, use the supported values in the *Time Zone Setting on Server* column.

Changes made to the system time zone from outside CiscoWorks applications might not be reflected in already-running CiscoWorks applications. After changing the time zone, restart all CiscoWorks applications.

Table 1   Supported Server Time Zones

Time Zone Acronym Setting on Device	Definition	Area Covered (Country/City)	Offset from GMT	Time Zone Setting on Server	Output in Report	
					GMT	Acronym
ACT	Australia Central Time	Australia/ Darwin	+9:30	Adelaide	GMT +9:30	ACT
AEST	Australia Eastern Standard Time	Australia/ Sydney	+10:00 +11:00 (DST)	Brisbane	GMT +10:00 GMT +11:00 (DST)	AEST
AET	Australia Eastern Time	Australia/ Sydney	+10:00	Brisbane	GMT +10:00 GMT +11:00 (DST)	AET

Table 1   ***Supported Server Time Zones (continued)***

Time Zone Acronym Setting on Device	Definition	Area Covered (Country/City)	Offset from GMT	Time Zone Setting on Server	Output in Report	
					GMT	Acronym
AHST	Alaska-Hawaii Standard Time	Hawaii/ Honolulu	-10:00	Hawaii	GMT -10:00	HST
ART	Argentina Standard Time	Argentina/ Buenos Aires	-3:00	Buenos Aires, Georgetown	GMT -3:00	ART ARST (DST)
ARST	Argentina Daylight Saving Time	Argentina/ Buenos Aires	-2:00	Buenos Aires, Georgetown	GMT -2:00	ARST (DST) ART
AST	Arabic Egypt Standard Time	Africa/ Cairo	+2:00 +3:00 (DST)	Cairo	GMT +2:00 GMT +3:00 (DST)	AST
BRT	Brazil Standard Time	Brazil/ Brasilia	-3:00	Brasilia	GMT -3:00	BRT BRST (DST)
BRST	Brazil Daylight Saving Time	Brazil/ Brasilia	-2:00	Brasilia	GMT -2:00	BRST (DST) BRT
CCT	China Coast Time	Asia/ Shanghai	+8:00	Beijing	GMT +8:00	CST
CDT	Central Daylight Time	United States/ Chicago	-5:00	Central Time	GMT -5:00	CDT (DST) CST
CET	Central European Time	Spain/Madrid	+1:00 +2:00 (DST)	Madrid	GMT +1:00 GMT +2:00 (DST)	CEST
CST	Central Standard Time	United States/ Chicago	-6:00	Central Time	GMT -6:00	CST CDT (DST)
CTT	China Taiwan Time	Asia/ Shanghai	+8:00	Beijing	GMT +8:00	CST
EAST	East Australian Standard Time	Australia/ Queens Island	+10:00	Brisbane	GMT +10:00	EAST
ECT	European Central Time	Europe/Paris	+1:00 +2:00 (DST)	Paris	GMT +1:00 GMT +2:00 (DST)	CEST
EDT	Eastern Daylight Time	United States/ New York	-4:00	Eastern Time	GMT -4:00	EST EDT (DST)
EST	Eastern Standard Time	United States/ New York	-5:00	Eastern Time	GMT -5:00	EST EDT (DST)

Table 1   Supported Server Time Zones (continued)

Time Zone Acronym Setting on Device	Definition	Area Covered (Country/City)	Offset from GMT	Time Zone Setting on Server	Output in Report	
					GMT	Acronym
FWT	French Winter Time	France/Paris	+1:00 +2:00 (DST)	Paris	GMT +1:00 GMT +2:00 (DST)	CEST
GMT	GMT Standard Time	Africa/ Casablanca	None	Greenwich Mean Time	GMT +0	GMT
HST	Hawaiian Standard Time	Pacific/ Honolulu	-10:00	Hawaii	GMT -10:00	HST
IRDT	Iran Daylight Time	Iran/Tehran	+4:30	Tehran	GMT +4:30	IRDT (DST) IRST
IRST	Iran Standard Time	Iran/Tehran	+3:30	Tehran	GMT +3:30	IRST IRDT (DST)
IST	Indian Standard Time	India	+5:30	Chennai, Kolkata, Mumbai, New Delhi	GMT +5:30	IST
JST	Japan Standard Time	Asia/Tokyo	+9:00	Tokyo	GMT +9:00	JST
MDT	Mountain Daylight Time	United States/ Denver	-6:00	Mountain Time	GMT -6:00	MDT (DST) MST
MET	Middle European Time	Spain/Madrid	+1:00 +2:00 (DST)	Madrid	GMT +1:00 GMT +2:00 (DST)	CEST
MEWT	Middle European Winter Time	Spain/Madrid	+1:00	Madrid	GMT +1:00 GMT +2:00 (DST)	CEST
MST	Mountain Standard Time	United States/ Denver	-7:00	Mountain Time	GMT -7:00	MST MDT (DST)
PDT	Pacific Daylight Time	United States/ Los Angeles	-7:00	Pacific Time	GMT -7:00	PDT (DST) PST
PST	Pacific Standard Time	United States/ Los Angeles	-8:00	Pacific Time	GMT -8:00	PST PDT (DST)
UTC	GMT Standard Time	Great Britain/ London	None	Greenwich Mean Time	GMT +0	GMT
VET/VST	Venezuela Standard Time	Venezuela/ Caracas	-4:30	Caracas	GMT -4:30	VST

Table 1 *Supported Server Time Zones (continued)*

Time Zone Acronym Setting on Device	Definition	Area Covered (Country/City)	Offset from GMT	Time Zone Setting on Server	Output in Report	
					GMT	Acronym
WDT	Western Daylight Time	Western Australia/ Perth	+9:00	Perth	GMT +9:00	WDT (DST) WST
WST	Western Standard Time	Western Australia/ Perth	+8:00	Perth	GMT +8:00	WST WDT (DST)
ZP4	Zone 3	Russia/ Moscow	+4:00	Not Supported	GMT +4:00	ZP4

Operating System Upgrade

While installing CiscoWorks LMS 4.0, the installation process checks for required patches. You must install:

- Any missing required patches, recommended patches, and cluster patches on Solaris systems.
- Required service packs on Windows systems

For a list of prerequisites, see Chapter 2 of *Installing and Migrating to CiscoWorks LAN Management Solution 4.0* at:

http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/install/guide/install.html

If CiscoWorks does not operate properly after you install all necessary patches or service packs, check the permissions in the directory i*nstall-directory*\objects\dmgt\ready. Local administrators group and casusers group must have full access.

If the permissions are incorrect, stop the Daemon Manager, change the permissions, and start the Daemon Manager again.

⚠️
Caution   If CiscoWorks LMS is running without the required service packs or patches, it will not function properly.

Server and Client Requirements

For information on server and client requirements for the system and browser, see Chapter 2 of *Installing and Migrating to CiscoWorks LAN Management Solution 4.0* at:

http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/install/guide/install.html

Caveats

This section explains:

- Using Bug Toolkit
- Open Caveats
- Resolved Caveats

Using Bug Toolkit

In CiscoWorks LMS 4.0 and later, use the Bug ToolKit to view the list of outstanding and resolved bugs in a release. This section explains how to use the Bug ToolKit through the following subsections:

- Search Bugs
- Export to Spreadsheet

Search Bugs

This section explains how to use the Bug ToolKit to search for a specific bug or to search for all the bugs in a specified release.

Step 1 Go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

You will be prompted to log into Cisco.com. After you login, the Bug Toolkit page opens.

Step 2 Click **Launch Bug Toolkit**.

Step 3 To search for a specific bug, enter the bug ID in the **Search for Bug ID** field and click **Go** in the **Search Bugs** tab.

To search for all the bugs in a specified release, enter the following search criteria in the **Search Bugs** tab:

- Select Product Category—Select **Network Management**.

- Select Products—Select **CiscoWorks LAN Management Solution** from the list.

- Software Version—Select **4.0** to view the list of outstanding and resolved bugs in CiscoWorks LAN Management Solution 4.0.

- Search for Keyword(s)—Separate search phrases with boolean expressions (AND, NOT, OR) to search within the bug title and details.

- Advanced Options—You can either perform a search using the default search criteria or define custom criteria for an advanced search. To customize the advanced search, select **Use custom settings for severity, status, and others** and provide the following information:

  – Severity—Select the severity level.

  – Status—Select **Open**, **Fixed**, or **Terminated**.

  Select **Open** to view all the open bugs. To filter the open bugs, clear the Open check box and select the appropriate sub-options that appear below the Open check box. The sub-options are New, Held, More, Open, Waiting, Assigned, Forwarded, Postponed, Submitted, and Information Required. For example, if you want to view only new bugs in CiscoWorks LAN Management Solution 4.0, only select **New**.

Select **Fixed** to view fixed bugs. To filter fixed bugs, clear the Fixed check box and select the appropriate sub-options that appear below the fixed check box. The sub-options are **Resolved** or **Verified**.

Select **Terminated** to view terminated bugs. To filter terminated bugs, clear the Terminated check box and select the appropriate sub-options that appear below the terminated check box. The sub-options are **Closed**, **Junked**, and **Unreproducible**. Select multiple options as required.

- Advanced—Select the **Show only bugs containing bug details** check box to view only those bugs that contain detailed information, such as symptoms and workarounds.

- Modified Date—Select this option if you want filter bugs based on the date on which the bugs were last modified.

- Results Displayed Per Page—Select the appropriate option from the list to restrict the number of results that appear per page.

Step 4 Click **Search**. The Bug Toolkit displays the list of bugs based on the specified search criteria.

Export to Spreadsheet

The Bug ToolKit provides the following options to export bugs to a spreadsheet:

- Click **Export All to Spreadsheet** link in the Search Results page under the Search Bugs tab. Specify file name and folder name to save the spreadsheet. All the bugs retrieved by the search will be exported.

- Click **Export All to Spreadsheet** link in the My Notifications tab. Specify file name and folder name to save the spreadsheet. All the saved bugs in all the groups will be exported.

If you are unable to export the spreadsheet, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1-800-553-2447).

Open Caveats

The open caveats describe possible unexpected behavior in CiscoWorks LAN Management Solution 4.0 release. These caveats may also be open in previous releases. You can get the details of:

- Open Caveats for CiscoWorks LAN Management Solution 4.0

- Open Caveats for CiscoWorks LAN Management Solution 3.2

Open Caveats for CiscoWorks LAN Management Solution 4.0

The caveats listed below in the table describe possible unexpected behavior in CiscoWorks LAN Management Solution 4.0 release. These caveats may also be open in previous releases. Bugs are listed in alphanumeric order by bug identifier.

Refer Using Bug Toolkit for querying and searching bug details.

This section contains:

- Open Caveats Related to User Interface and Browsers in LMS 4.0
- Open Caveats Related to Monitoring and Troubleshooting in LMS 4.0
- Open Caveats Related to Configuration and Work Centers in LMS 4.0
- Open Caveats Related to Discovery and Device Management in LMS 4.0
- Open Caveats Related to Administration in LMS 4.0
- Open Caveats Related to Portlets and Dashboards in LMS 4.0
- Open Caveats in CiscoWorks LAN Management Solution 4.0.x Windows 2008 R2 Patch

Open Caveats Related to User Interface and Browsers in LMS 4.0

Table 2 lists the open caveats related to User Interface and Browsers in LMS 4.0.

Table 2   Open Caveats Related to User Interface and Browsers in LMS 4.0

Identifier	Headline
CSCsv54697	Error occurs when you select multiple records in dashboards
CSCte18816	PDF export does not work in CiscoWorks page in IE 7.0
CSCtf16971	Unable to export report to CSV in IE 7.0 and 8.0 browsers
CSCtf80741	Text box hover color is not be visible in IE.
CSCtg08831	In Template Center, text box acts like a browse button
CSCth08575	Unable to launch Help in new browser window or tab
CSCth35862	Telnet Action Item for Device mouse hover does not work in IE.
CSCth37535	Unsupported browser popup appears for 64 bit Firefox browser
CSCth59316	Access arrow is hidden when there is long text with or without ellipsis.
CSCth79619	Inconsistency in icons.
CSCth87484	Row selection not retained when you sort the columns with more than 25 rows.
CSCtf00121	Confirmation window does not appear when you navigate from one page to another.
CSCte61659	In tree selectors, partial selection of the parent does not appear when any child node is selected.
CSCsm31620	Mismatch in the number of devices in the DCR device selector and other pages
CSCti74142	After a session timeout, error message appears in some pages in Work Centers
CSCti80788	When you click the device hyperlink in High Severity Alerts and High CPU Utilization portlets, you cannot launch help for the troubleshooting pages.

Open Caveats Related to Monitoring and Troubleshooting in LMS 4.0

Table 3 lists the open caveats related to Monitoring and Troubleshooting in LMS 4.0.

Table 3   *Open Caveats Related to Monitoring and Troubleshooting in LMS 4.0*

Identifier	Headline
CSCsz30292	For IPv6 addresses, warning or error messages do not appear for unsupported modules in Device Centre
CSCte56601	System report does not have the color scheme of LMS 4.0
CSCtf53724	Error occurs when you refresh Device and Fault views
CSCtf69125	Cleared events count does not appear in the Info icon.
CSCtf78256	Unable to generate some reports for some roles
CSCtf93056	Unable to filter Device Performance Management events
CSCtg27046	Topology image appears on the left of the page during loading
CSCtg30117	After you delete devices from DCR, Fault Monitor triggers cleared events
CSCtg30144	Hyperlink does not appear for topology links
CSCtg32087	Proper error messages do not appear in NAM portlets
CSCtg73655	Proxy Traceroute is in loading state for long time
CSCtg84633	Error message appears when you click device selector icon
CSCtg94098	Reachable and unreachable status appears in device availability portlet.
CSCtg98830	When you click a device in Topology, an error appears in the device tab.
CSCtg98859	In Topology view, when we click a device, data appears in the Device Tab after a long time.
CSCth01120	In Topology, unable to click the link when the display name is long for endhost
CSCth13276	Script error appears when you launch the troubleshooting page
CSCth15687	Selected device does not appear in topology view
CSCth18282	In Fault Monitor, unable to find Unidentified trap event of unmanaged devices.
CSCth38302	In the collector summary portlet, the latest Data Collection value does not appear
CSCth41803	Unable to launch the report for deleted and unmanaged devices in Event Monitor
CSCth57108	Problems in UI components when you launch Fault Monitor or Event Monitor in IE with Win 2003 or 2008
CSCti05592	In Troubleshooting workflow, unable to enter IP address in device field
CSCti15148	In Fault Monitor, there are no icons for groups, and an error occurs when you annotate device with text in double quotes.
CSCti40318	Discrepancies in IPSLA and Device Performance Management tasks
CSCti45503	Loading symbol does not appear in IE when you select all devices in 5K SKU
CSCti67873	Blank spaces appear in the Event Monitor grid
CSCth18870	In Japanese OS Windows Server 2008 Enterprise, unwanted characters appear in the ping and traceroute outputs

Table 3   Open Caveats Related to Monitoring and Troubleshooting in LMS 4.0 (continued)

Identifier	Headline
CSCth59941	In Fault Monitor, server side filtering and sorting does not work for the Owner column
CSCth07002	Discrepancies in listing the MIB variables in the Performance Custom Reports.
CSCth94419	When you own, clear, or annotate events and click the Yes button multiple times, multiple events occur
CSCth96491	Reload of report creation page duplicates the last job
CSCti78790	When we launch the Event Monitor from the Fault Monitor page, with 5K devices, Device Fault Summary view takes a long time to load.
CSCtg30108	Event Monitor does not differentiate the user-defined device groups and user-defined fault groups, and displays only one user-defined group.

Open Caveats Related to Configuration and Work Centers in LMS 4.0

Table 4 lists the open caveats related to Monitoring and Troubleshooting in LMS 4.0.

Table 4   Open Caveats Related to Configuration and Work Centers in LMS 4.0

Identifier	Headline
CSCtf48249	Unable to purge Identity Data using the UI.
CSCti77576	In Identity, after you sort ports, the enable Identity commands are deployed on the wrong ports
CSCtg38171	Trunk creation in create VRF flow fails.
CSCtg78557	In Template Center, error message does not appear when you select conflicting templates
CSCtg80037	Reset button does not work properly in the bug summary report
CSCtg80182	WebAuth data is not updated in embuindentity table.
CSCtg98303	Excluded ports appear in quick report created with port group
CSCti77485	Software update page link is missing in RSAC server
CSCth04990	Blank page appears when you access the unauthorized pages of Work Centers
CSCth07400	After creating VLANs, the device selector in the Modify Trunk Attributes shows duplicate devices.
CSCth15494	When you change the state of an unmanaged device to managed state, the poller, threshold and trendwatch details are not updated
CSCth84393	Error message appears in EnergyWise pages
CSCti15058	Discrepancies in Event Forensics page
CSCti16034	Image distribution through SCP fails in mixed stack
CSCti39064	Unable to create device groups using the attributes such as System.ASP_capability, System.Identity_Capability and System.Smart_Install_Directors
CSCti48096	Blank page appears when you generate the Device Performance Management Interface Report

Table 4   Open Caveats Related to Configuration and Work Centers in LMS 4.0 (continued)

Identifier	Headline
CSCti61713	In the failed or succeeded archive inventory report, an error message appears when you click the export device list to device selector
CSCti70528	Errors appear in the EnergyWiseDeviceII table and collection log
CSCti71869	VRF collection remains at Running state
CSCti72089	Minus zero appears in EnergyWise cost savings report and total savings portlet
CSCti83166	After restoration of a selective backup, Templates in Template Center do not appear.
CSCtw51607	Device under NAT environment is not collected in EnergyWise.

Open Caveats Related to Discovery and Device Management in LMS 4.0

Table 5 lists the open caveats related to Discovery and Device Management in LMS 4.0.

Table 5   Open Caveats Related to Discovery and Device Management in LMS 4.0

Identifier	Headline
CSCsy81588	Discrepancy in the DCRDevicePoll job end time in job browser and mail.
CSCsz79602	Default credentials are not used when you import devices from LMS 3.x
CSCta13362	Discovery adds wrong device type, and shows device count with CDP and Cluster
CSCta13397	IPV6 subnet masks are not validated in ping sweep seed device settings.
CSCta66989	Discovery configuration XML files are not updated with latest MAC address
CSCte60815	DCRDevice Poll using ICMP wrongly shows devices as Unreachable
CSCte71680	UDM Device Management Policy does not work properly for Private Groups
CSCtg83979	Subnet-based groups appear under System-defined groups in UDM group selector.
CSCtg41303	Device moves to managed state automatically and triggers Data Collection.
CSCti64982	UDM policy is not disabled after DCR Slave (S1) is restored in Standalone server.
CSCti67131	After LMS 2.6 SP1 restore, the all devices option is updated in UDM.
CSCsz79649	In Solaris 5K server, the CTM registry gets corrupted and an error appears.

Open Caveats Related to Administration in LMS 4.0

Table 6 lists the open caveats related to Administration in LMS 4.0.

Table 6   Open Caveats Related to Administration in LMS 4.0

Identifier	Headline
CSCsf01047	Security Vulnerability: Files under CSCOpx can be overwritten through DCR
CSCsh54838	Performance issues with device selector having more no of devices
CSCsv97838	Errors appear in collect server information
CSCsx60915	Log4j does not rotate logs in windows
CSCta06026	Unable to sort unreachable device report after applying a filter
CSCtd31272	Unable to connect with OGS CLI when the Solaris server is in SSL mode.
CSCti00325	The Import Group window does not close after import completes successfully
CSCte29226	Redirection errors appear when you login to LMS, with browser in protected mode, on Windows 2003 and 2008
CSCti76696	During pre-installation, error message appears before a successful installation
CSCte57739	File Copy In Progress popup that appears during installation does not have a minimize button
CSCte69340	Error messages appear in install.log
CSCte77294	Column sorting not working for Device Type Count under Device Update
CSCtf45257	Multiple spaces in username is saved with a single space
CSCtf50914	Validation is not done when the password length is not in accordance with the with policy settings.
CSCtf52519	Install Shield crashes while uninstalling CSM
CSCtf82773	Processes do not start due to port bind exception.
CSCth20366	For a 5K SKU, in the job browser, the status of a successful discovery job appears as Daemon manager not responding.
CSCth46519	Creating Default Credential set is not intuitive
CSCth87333	Error appears when you exclude all the device in Groups
CSCti02289	Device polling gets stuck
CSCti67125	Groups imported in master do not appear in slave and the members are not updated
CSCti71890	VRF-Lite purge job fails when you modify the purge policy
CSCti74728	Unable to login using the username "default" with any role

Open Caveats Related to Portlets and Dashboards in LMS 4.0

Table 7 lists the open caveats related to Portlets and Dashboards in LMS 4.0.

Table 7   Open Caveats Related to Portlets and Dashboards in LMS 4.0

Identifier	Headline
CSCtf18800	Default layout is disabled when you change the dashboard type
CSCth40388	In a Windows server with 5K SKU, Tomcat creates Out of Memory error in PermGen
CSCth97754	Display order is not proper in manage dashboards
CSCti25379	When you login with a username having special characters and launch manage dashboards, a page appears with a blank dashboard.
CSCti52645	In Work Centers multi-instance portlets which use sliders, the value of the slider changes when you refresh or maximize the portlets.
CSCti74508	Unable to view and add portlets when you rename the default dashboards.
CSCti80562	Unable to save configuration data in N-Hop View, Identity-802.1x Agentless Users, and, Identity-Authenticated Users portlets.
CSCti75696	Unable to enable debugging for Getting Started from the UI
CSCti80845	Null pointer exception occurs when you modify My Profile in Getting Started with a different authentication mode

Open Caveats in CiscoWorks LAN Management Solution 4.0.x Windows 2008 R2 Patch

Table 8 lists the open caveats in CiscoWorks LAN Management Solution 4.0.x Windows 2008 R2 Patch

Table 8   *Open Caveats in CiscoWorks LAN Management Solution 4.0.x Windows 2008 R2 Patch*

Bug ID	Summary	Explanation
CSCtl22181	If you are trying to abort the LMS 4.0.x. R2 patch installation that is currently running, the installable takes some time to quit.	If you are trying to abort the LMS 4.0.x. R2 patch installation that is currently running, the installable takes some time to quit. Meanwhile when you try to click the installable again, a message appears that another instance of installation is running. This problem occurs in the following scenarios: • Installing LMS 4.0.x patch versions without installing LMS 4.0 • Installing LMS 4.0.x using Windows 2008 R2 patch and aborting the installation immediately. Workaround: Kill the CiscoWorks_LMS_4.0.x_WIN2K8_R2.exe process using Task Manager.
CSCtl22181	Error while launching NMIC.	When you launch "Change Integration" option, the following error message appears: `Cannot start Change Integration options.` Workaround: Login as administrator and try again.
CSCtl22280	R2 patch is not applied when installing LMS 4.0 through R2 installable.	When you install LMS 4.0 through R2 installable in Windows 2008 R2 server, installation of LMS 4.0 gets completed but DfmBroker process does not start. Workaround: You have to disable the virus scanner on your system during the installation.

Open Caveats for CiscoWorks LAN Management Solution 3.2

The caveats listed in the tables below describe possible unexpected behavior in CiscoWorks LAN Management Solution 3.2 or earlier releases. Bugs are listed in alphanumeric order by bug identifier.

Refer Using Bug Toolkit for querying and searching bug details.

This section contains:

- Open Caveats in CiscoWorks Common Services 3.3
- Open Caveats in CiscoWorks Resource Manager Essentials 4.3

- Open Caveats in CiscoWorks Campus Manager 5.2
- Open Caveats in CiscoWorks Device Fault Manager 3.2
- Open Caveats in CiscoWorks Internetwork Performance Monitor 4.2
- Open Caveats in CiscoWorks Health and Utilization Monitor 1.2

Open Caveats in CiscoWorks Common Services 3.3

Table 9 lists the open caveats in CiscoWorks Common Services 3.3.

Table 9   Open Caveats in CiscoWorks Common Services 3.3

Identifier	Headline
CSCdr24473	Cannot invoke Pathtool application from NMS for Integration Utility.
CSCdr41597	There is no support for device-specific application integration with NMS.
CSCin28182	The Integration Utility Adapter window does not display the description of the adapters properly.
CSCin80600	Temporary files created while integrating CiscoWorks with NMS are not removed after integration
CSCsa51353	Network Management Information Center (NMIC) does not exit during integration.
CSCsa57080	In Solaris, temporary files remain even after the Integration Utility is uninstalled.
CSCsb84839	No option to configure proxy server settings in Integration Utility.
CSCsc38944	Problem occurs while integrating HPOV 7.5 with CiscoWorks applications.
CSCsg97728	Some scheduled jobs are moved to Missed Start state or rescheduled for the next run.
CSCsh36085	Tomcat logs are not rotated properly.
CSCsh49922	Cannot use Telnet to connect to a device from the Device Center.
CSCsk15483	Any error that occurs while configuring seed devices is not displayed in the user interface.
CSCsk17402	An error occurs on LMS server because the certificate has expired.
CSCsk35018	Database engines supports broadcast clients and open UDP ports to listen for client broadcasts.
CSCsk44387	In Solaris, logging into `dcrcli` fails when the username contains special characters.
CSCsk46142	The Job Details popup window for DCR jobs displays the wrong start time.
CSCsk55579	Problem occurs in daily job schedules before and after the DST patch installation.
CSCsk57503	Daily jobs scheduled in the DST timings as the second instance, run as the first instance.
CSCsl00295	NMIC application version displayed in HP Open View is incorrect.
CSCsl13291	Some of the SNMP properties are not migrated from Campus Manager Device Discovery to Common Services Device Discovery.
CSCsl60984	Some MIBs are not completely loaded while integrating CiscoWorks with NetView.
CSCsm07813	Scheduled Software Download jobs deleted from Software Center Event logs are not deleted from Job and Resource Manager.
CSCso62148	Found By Modules field in Discovery reports display incorrect entries for CDP and Routing Table modules.

Table 9   Open Caveats in CiscoWorks Common Services 3.3 (continued)

Identifier	Headline
CSCso84279	Proper error messages do not appear in Object Finder portlet.
CSCsq31632	In Windows, close buttons and text fields do not work properly in the CiscoWorks installation window.
CSCsq52863	Long component names that do not contain spaces, are not wrapped within a HTML scrolling table.
CSCsq52970	The `userdns` attribute is not migrated from LMS 2.6 or LMS 3.1 to Common Services.
CSCsv67482	The Found By Modules for Global seed devices appear incorrectly.
CSCsw36484	The Groups Administration page is not refreshed after groups are imported.
CSCsw65064	Although the CiscoWorks users are not authorized to import the groups to other CiscoWorks applications, the groups are imported successfully.
CSCsw73069	Job and Resource Manager displays different status for scheduled jobs.
CSCsw80572	The Log Space Portlet in Common Services view shrinks the browser window.
CSCsw96615	The confirmation message on Export Devices to File task completion does not appear in the user interface.
CSCsx55534	An error message appears while the Immediate backup is running.
CSCsy03756	Device added with blank image icon in Device Selector.
CSCsy19579	Discovery seed devices are added to wrong Device Discovery modules.
CSCsy31948	CiscoWorks does not launch from Windows 2008 client.
CSCsz07363	In Windows, the LicenseServer process goes down and creates a hs_err file.
CSCsz30292	Device Center does not display warning or error messages for modules that do not support IPv6.
CSCsz89760	Online backup of data fails occasionally.

Open Caveats in CiscoWorks Resource Manager Essentials 4.3

Table 10 lists the open caveats in CiscoWorks Resource Manager Essentials 4.3.

Table 10   Open Caveats in CiscoWorks Resource Manager Essentials 4.3

Identifier	Headline
CSCdm87814	Check Contract Status information is generated only for Cisco IOS devices.
CSCsa16772	Unable to create private custom template with same name for different users
CSCsa17529	Special characters such as single quotes, are not supported in a report template name.
CSCsa22899	When you provide only the enable password, and not the Telnet username and password, Device Credential Verification displays Did Not Try message
CSCsa28210	Software Identity is missing in DEE XML for CSS 11800 devices.
CSCsa29037	Image upgrade using Remote Stage fails if the image size exceeds 32 MB.
CSCsa33492	Change Audit report does not export the grouped records.

Table 10   Open Caveats in CiscoWorks Resource Manager Essentials 4.3 (continued)

Identifier	Headline
CSCsa36845	Processor Port and Module Port section are missing from Detailed Device Report for 4506 IOS.
CSCsa38526	Processor details like RAM and NVRAM Information is duplicated for some multi-processor devices in Detailed Device Report.
CSCsa45574	Alias detection does not work for devices accessed via a virtual management IP address.
CSCsb42968	RCP does not work for Windows 2003 Server.
CSCsb78495	A Config Editor job in the overwrite mode does not work for PIX devices.
CSCsb82197	A Config Editor deploy job fails when set length command is downloaded manually in Merge or Overwrite mode.
CSCse03788	Audit Trail report for deleted devices is not proper.
CSCse08118	SWIM distribution.xml shows incorrect IP address in dual home server.
CSCse18070	For IGESM devices, verification fails with the message that RAM on device is not sufficient to proceed with Software image distribution.
CSCse26973	For IGESM devices, the NVRAM and Total RAM details are missing in the Hardware report.
CSCse38083	Incompatible images are recommended during Software distribution for MDS9500 devices.
CSCse53270	Undo does not work for successful image distribution jobs for IGESM and 2960G devices.
CSCse54126	Software Distribution and Upgrade Analysis flows show devices twice in the reports.
CSCse56927	Software Distribution by device fails when you use RCP for 2960 devices.
CSCse63584	Software Distribution by device (Advanced) fails when you use RCP for IGESM devices.
CSCsh36359	Write2Start command does not work properly for PIX devices.
CSCsh65909	Write2Start does not work properly for MDS devices.
CSCsi53367	Booting of device fails when IOS image upgrade is done through Software Management.
CSCsi59716	Configurations edited in Processed mode do not support Write2Start.
CSCsk42108	RME is unable to copy the image file from the device to the server if the Flash card has been replaced on the device.
CSCsm02177	Some Attributes either do not appear or appear as N/A or Inventory not collected in Custom Inventory Reports if they are Null or empty in database.
CSCsm63267	Image recommendation fails for a software distribution job, when some image features are not retrieved from Cisco.com
CSCsm67165	Inventory Fetch does not happen after a software image upgrade and subsequent reload of a device.
CSCso66555	Total RAM size in Hardware and Detailed Device reports differs for 6509-E/6509-VE devices
CSCsq14383	All profiles created for Call Home get listed under a single profile configlet.

Table 10   Open Caveats in CiscoWorks Resource Manager Essentials 4.3 (continued)

Identifier	Headline
CSCsq14383	All profiles created for Call Home get listed under a single profile configlet.
CSCsx47363	Port and module groups do not work correctly if the parent device group is modified.
CSCsy23183	Selective backup data includes stale entries
CSCsy76335	Configuration commands appear as banner
CSCsz45971	Software Management repository location is set to the default path when upgrading to RME 4.3
CSCsz50487	Reports archives are not restored, and purge jobs are not backed up.
CSCsz83555	If a PIX or ASA having 8.x code or higher is upgraded in SWIM using SSH, the job fails
CSCtc44598	In RME 4.2 and RME 4.3, the list of images in SWIM is not filtered according to the Image Recommendation settings
CSCtd67173	In RME 4.3 and RME 4.3.1, SNMPv3 credential verification fails for ASA devices having 8.2(1) image
CSCte89885	RME Inventory collection fails for Blade Switch 3120X
CSCtg45161	In RME 4.3.1, unable to view Compare Config results of Base Config versus Latest Version of Multiple Devices in IE 7.0
CSCtg51646	Contract Connection does not work with a large number of devices
CSCth43286	When you add, edit, or update devices in DCR using any user ID, admin is logged as the user for the events
CSCti42219	RME Compliance shows non-compliant devices like ATM subinterfaces as compliant devices
CSCti46336	Multi-service port report on 6500 VSS shows only 3 out of 4 power supplies
CSCti51188	WLC devices do not work with Contract Connection

Open Caveats in CiscoWorks Campus Manager 5.2

Table 11 lists the open caveats in CiscoWorks Campus Manager 5.2.

Table 11   Open Caveats in CiscoWorks Campus Manager 5.2

Identifier	Headline
CSCdm83204	Campus Manager applications do not work when you access CiscoWorks using `http://`*localhost*`:1741`
CSCdp76410	Campus Manager client cannot connect to server using proxies.
CSCdp88318	Link attributes are not updated after a change is made.
CSCdr85384	Phone entries displayed by User Tracking differ from entries displayed by Cisco CallManager.
CSCds88388	Cannot launch CiscoView on an IGX series device.
CSCdt06183	User Tracking Main Table may not display all entries that are displayed in the phone table.

Table 11   Open Caveats in CiscoWorks Campus Manager 5.2 (continued)

Identifier	Headline
CSCdt18293	Visio drawing does not import cleanly into Microsoft Visio.
CSCdt25525	User Tracking Main Table sometimes displays CDP-enabled devices that are outside the ANI discovery boundary.
CSCdt27824	Entire list of ports in a VTP domain appear when you select certain Transparent VTP domains from the VLAN Assignment dialog box.
CSCdt50619	Two devices, connected by multiple links, appear to be connected by only one link.
CSCdw04486	End hosts not discovered with Catalyst 2950 running a software release earlier than Cisco IOS Release 12.0(5)WC2.
CSCdw04499	End hosts are not discovered with Catalyst 3550 running Cisco IOS Release 12.1(6)EA1 or earlier.
CSCdw09818	Port Attribute in VLAN Port Assignment displays incorrect information.
CSCdw67129	Topology Services cannot resolve the hostname of newly discovered devices.
CSCea39271	Topology Services displays the devices connected to a UB Token-Ring Hub in the Unconnected Devices View.
CSCeb68819	Topology Services does not display dual links.
CSCed72194	MST device report does not report CIST root correctly.
CSCef67937	Campus Manager does not show port as trunking if the port is part of the Channel.
CSCin00181	Last Seen field gets updated for disconnected IP phones.
CSCin00363	End host does not appear if obsolete device IP address is assigned.
CSCin22459	Topology Groups membership update does not work as expected.
CSCin27895	Topology Services does not show VLANs as active, if the switch is in NULL folder under VTP Domain.
CSCin29281	Device Attribute of Cisco Catalyst 6000 devices does not display the IP address.
CSCin33112	Cannot delete devices on a remote system in SSL mode using the command line interface.
CSCin43965	Spanning Tree reports more than one root for a switch cloud.
CSCin45070	Launch points do not work if http/https ports have other than the default value.
CSCin45496	Campus Manager does not report UDLD discrepancy for Cisco Catalyst 2900 series switches.
CSCin46370	Trunk Negotiation Enabled Discrepancy Report does not show the Trunk mode details of the ports of some devices.
CSCin46405	Campus Manager does not report Spanning Tree discrepancies for some devices.
CSCin46641	Campus Manager does not calculate Trunk mode related discrepancies.
CSCin48159	Cannot launch IDSM from Service Modules launch point for IDSM2 card of Cisco Catalyst 6000 device.
CSCin67279	Community suffix support is not available for MST on Cisco IOS switches.

Table 11 Open Caveats in CiscoWorks Campus Manager 5.2 (continued)

Identifier	Headline
CSCin68983	Cannot configure Trunk between Catalyst 2900XL and Catalyst 3500XL devices.
CSCin74855	Devices are not managed in Campus Manager if management IP is not in ACS.
CSCsa04026	Link line or connection between two devices gets warped, if one device is moved.
CSCsa09287	Cannot map VLANs to instance if the device runs MISTP.
CSCsa10216	Incorrect VTP version displayed in VTP reports.
CSCsa11888	Channel or Trunk cannot be configured because of STP recalculation.
CSCsa12292	VLANs are not loaded for STP Offline Computation.
CSCsa12292	VLANs not loaded for STP Offline Computation.
CSCsa14652	NAM and IDS Modules appear as end hosts in User Tracking.
CSCsa18405	In PVLAN configuration, the secondary VLAN creation and association to Primary VLAN fail on Cisco Catalyst Operating System version 8.1.
CSCsa20659	Purge Job is created although you delete it from User Tracking Report Jobs.
CSCsa20827	Subnet based groups are not deleted from Campus Manager Topology Groups although you delete them from DCR.
CSCsa22699	Inter-VLAN Routing configuration user interface (UI) does not differentiate primary and secondary IP addresses.
CSCsa22708	Campus Manager does not manage existing devices when you upgrade from higher device limit to lower device limit.
CSCsa25203	Campus Manager does not generate Time Domain Reflectometry (TDR) Report for Cisco 3750 and Cisco 4000 series switches.
CSCsa27118	User Tracking Report displays Port State as Static for dot1x authenticated ports.
CSCsa27318	Topology Services displays an error, `OutOfMemoryError`, while working with 3000 devices.
CSCsa97284	UT-Lite drops packets when data is sent at a high rate.
CSCsb17074	User Tracking does not discover hosts connected to devices with SNMPv3 credentials.
CSCsc24255	Improper error message while configuring IVR.
CSCsc24275	VLAN interfaces created through IVR are not shown in the existing interface list for that device.
CSCsc43106	Device not discovered if SysUpTime is masked.
CSCsd58215	DNS resolution for end user entries takes an inordinate amount of time.
CSCse26688	Cannot launch Device Attributes report for more than 3000 devices.
CSCse39112	Rules created for Groups in Campus Manager do not work properly.
CSCse57193	Campus Manager does not resolve hostnames for endhosts added through SNMP traps in DHCP environment.
CSCse68687	DNS timeouts do not happen as per the timeout value set.
CSCsg92439	Campus Manager does not compute the correct number of instances, when there are redundant links between switches.

Table 11 **Open Caveats in CiscoWorks Campus Manager 5.2 (continued)**

Identifier	Headline
CSCsh20449	RMON configuration fails on Cluster Member switches.
CSCsh41208	Topology Services does not support deleting 1000 devices at a time.
CSCsh71141	N-Hop View Portlet shows wrong device icon for MSFC Switch.
CSCsh85533	Exporting User Tracking data through Data Extraction Engine results in an Out of Memory error.
CSCsi11610	Background image cannot be set if the image name has spaces in it.
CSCsi21974	Exporting port attributes report crashes the browser.
CSCsi30755	Ports are not listed properly when shared VLANs are deleted.
CSCsi54994	Launching printer friendly format of End host report takes a long time.
CSCsi56555	PVLAN is not created after ANI server restart.
CSCsi85533	Wrong error message displayed when you try to create VLANs in VTPv3 server.
CSCsm25505	Device Attribute and VLAN report fails when more than 200 devices are selected.
CSCso87643	Topology services displays unauthorized devices
CSCsq55637	In VSS mode, the User Tracking report does not display the endhosts connected to standby devices.
CSCsu84974	UT Acquisition does support invalid UTF-8 character for Port Name and Device Name fields.
CSCsw36595	The values you enter in the VLAN to VRF Mapping page are deleted if you click the Toggle icon.
CSCsw39443	The Default Sort option for scheduled jobs is not supported.
CSCsw45726	The Device Center page does not display the reports generated by VNM.
CSCsw63053	The VNM Home page displays a VRF without an RD value with device count as zero. VRF without RD value, is an improper configuration.
CSCsw74869	You can launch VNM from the Layer 2 devices in Topology Services.
CSCsw80285	In the Edge VLAN Configuraton workflow, if you assign a null VLAN to a VRF, the VLAN to VRF Mapping page does not list the virtual interfaces for the null VLAN.
CSCsw84667	The devices deleted in the ACS server are not reflected in the Topology Map View.
CSCsw90100	Automatic Refresh option of Topology Services at the client side, does not work as expected.
CSCsy29024	If you Campus Manager uninstall process is not removing the log files and jobs
CSCsz15769	UT Custom report jobs are not shown if custom templates are deleted.
CSCsz23980	In LAN Edge view, the application throws a NullPointer exception in Java console.
CSCsz55346	In VNM home page, page number validation is not happening in VRF LIST paging table.

Open Caveats in CiscoWorks Device Fault Manager 3.2

Table 12 lists the open caveats in CiscoWorks Device Fault Manager 3.2.

Table 12   Open Caveats in CiscoWorks Device Fault Manager 3.2

Identifier	Headline
CSCsq60989	Check point and null pointer exceptions appear in the daemons.log
CSCsu01718	Devices get stuck at 70% Learning state.
CSCsw48433	When you restart the daemons and launch the Event Sets UI before 15 mins, the UI will be blank.
CSCsw98711	When devices are not reachable, ICMP and SNMP requests are found during Rediscovery.
CSCsw98735	After a rediscovery of devices, DFM Incharge Engine polls the SNMP timed out devices.
CSCsx72359	With 1500 SNMPv3 devices, SVNMP requests are skipped when polling interval is set as 60 seconds.
CSCsy34104	During E-mail configurations, e-mail IDs are not properly validated.
CSCsz13416	Problems in performance occur with 200 groups
CSCsz13696	The report printed using the Print Friendly button in the Device Details page displays only 2000 records.
CSCsz21403	Cannot create User-defined groups if DFM has Voice and Telephony devices.
CSCsz28940	The Detailed Device View page displays the MSFC device as Suspended when you delete its parent device.
CSCsz77669	When you add new devices to a group in Common Services, the devices are not as automatically selected in DFM Notification Groups.
CSCsz77669	Device Selection does not appear when you edit a Notification Group.
CSCsz79389	DFM Groups are not created or updated when devices are deleted and added again.
CSCta11852	Discovery does not work when VPN concentrator devices are added
CSCtd91333	In Catalyst 4500 Dual Supervisor configuration, you cannot see the status updates in DFM, when you change from active to standby SUP.
CSCtf47441	For ACE 4710, DFM does not use the ENTITY-SENSOR-MIB for environment data.

Open Caveats in CiscoWorks Internetwork Performance Monitor 4.2

Table 13 lists the open caveats in CiscoWorks Internetwork Performance Monitor 4.2.

Table 13   Open Caveats in CiscoWorks Internetwork Performance Monitor 4.2

Identifier	Headline
CSCsh59293	IP SLA probes are not deleted when you restore data.
CSCsh60910	Backup-Restore of same version overwrites the default DNS operation
CSCsh98268	Statistical data of PathEcho collectors are not migrated while migrating from IPM 2.6 to IPM 4.x.
CSCsm87616	The probes do not get deleted from the source device and the uninstallation fails if the IPM process is down during uninstallation.
CSCso61456	While importing a collector, a new operation is created and MIBs are set to the default values.
CSCso97007	When you upgrade to IPM 4.1, the Action Event is not set as Immediate for timeout
CSCsz54494	Delay in the polling interval of collectors.
CSCth21594	Missing hourly data collection occurs for some Echo-based Collectors.
CSCti65644	When you create a collector with the & character in the collector name, an error appears in the Realtime data graph.
CSCti77722	Unable to sort System reports based on date.

Open Caveats in CiscoWorks Health and Utilization Monitor 1.2

Table 14 lists the open caveats in CiscoWorks Health and Utilization Monitor 1.2.

Table 14   Open Caveats in CiscoWorks Health and Utilization Monitor 1.2

Identifier	Headline
CSCsj35878	If you edit or copy a template that you created using a newly loaded MIB, it does not display the MIB file in the Show MIB drop-down list.
CSCsk61569	PDF generation fails if a report has large amount of data.
CSCsv88040	HUM does not work properly if there are multiple interfaces with the same name.
CSCsw71763	The change in variable name is not reflected in the configured thresholds.
CSCtb53068	HUM UI shows No Data Found message when a large number of pollers are managed
CSCti77773	CPU Utilization template instances and the value of the MIB variable EntPhysicalDescrare are null for Cisco7609.

Resolved Caveats

This section contains Resolved Caveats in LMS 4.0.

Resolved Caveats in LMS 4.0

The caveats listed in Table are caveats of the different applications of LMS 3.2 resolved in LMS 4.0.

Refer Using Bug Toolkit for querying and searching bug details.

This section contains:

- Caveats of RME 4.3 Resolved in CiscoWorks LMS 4.0
- Caveats of CS 3.3 Resolved in CiscoWorks LMS 4.0
- Caveats of CM 5.2 Resolved in CiscoWorks LMS 4.0
- Caveats of DFM 3.2 Resolved in CiscoWorks LMS 4.0
- Caveats of IPM 4.2 Resolved in CiscoWorks LMS 4.0
- Caveats of IPM 4.2 Resolved in CiscoWorks LMS 4.0
- Caveats of HUM 1.2 in CiscoWorks LMS 4.0

Caveats of RME 4.3 Resolved in CiscoWorks LMS 4.0

Table 15 lists the caveats of RME 4.3 resolved in CiscoWorks LMS 4.0.

Table 15 Caveats of RME 4.3 Resolved in CiscoWorks LMS 4.0

Identifier	Headline
CSCsd97751	In RME 4.0.3, Unable to enter a value less than 5 in the TFTP timeout field of Device Attributes.
CSCsl16539	Software Management job takes a long time to detect that a reboot of the device has not been successful, after downloading a new image.
CSCsz32320	Syslog Message Report of Device Center shows only messages from a week ago or older.
CSCsz36795	Baseline compliance jobs fail with the following error: `CM0152 Prerequisite Commands does not exist in device archive.`
CSCsz41441	Cannot upgrade an 880 series router if RME manages the router with SNMPv3 credentials.
CSCsz58112	RME 4.2 Netshow command fails on ASA.
CSCsz91572	RME associates config changes to the wrong username.
CSCta05277	Inventory collection fails with an RICS0001 error.
CSCtb16925	
CSCta08895	RME fails to fetch the config from PIX OS devices running in security context mode.
CSCta12604	EOX and PSIRT report job objects contain CCO credentials.
CSCta13429	RME fetches the `show running brief` command from devices
CSCta23723	EoS/EoL report fails saying unable to connect to Cisco.com

Table 15   Caveats of RME 4.3 Resolved in CiscoWorks LMS 4.0 (continued)

Identifier	Headline
CSCta26477	RME is unable to import images from CatOS devices
CSCta28992	SWIM job purge deletes scheduled jobs.
CSCta32423	RME documentation does not explain restrictions on syslog backup directory.
CSCta73609	Need to update documentation for Remote Syslog Collector support.
CSCta76147	Unable to get the EoS/EoL report via Proxy server.
CSCta76844	Config Quick Deploy jobs in overwrite mode may not find any differences between the archive to be deployed and the current archive, and does not deploy config changes to the device.
CSCta76898	Unable to upgrade Cat 6500 from 12.1E to 12.2SX.
CSCta80687	Baseline Template does not evaluate negative prerequisites that use a RegEx match.
CSCta85094	Config Quick Deploy in overwrite mode incorrectly deletes child commands.
CSCtb00572	RME database cache size becomes too large
CSCtb06637	RME cannot perform inventory collection for VNP 3000 devices
CSCtb11894	Hardware Inventory Report shows the wrong serial number listed against a Catalyst switch when multiple switches are stacked.
CSCtb20549	For multihomed servers, RME detects the server IP using only TELNET/SSH protocol.
CSCtb42198	Unable to check for compliance when a baseline contains prerequisite child commandlets.
CSCtb54944	For Cat 7600, incorrect protocol is documented in SDT for transfer of images
CSCtb55607	Unable to fetch configs from GSS devices
CSCtb76998	Baseline comparison jobs which run with cwcli `comparewithbaseline` command fail.
CSCtb94231	Device Credential Verification report results for PIX and Security Context devices are misleading.
CSCtc18888	Syslog automated actions are not triggered; however, syslog messages are written to the RME database, and do appear in the syslog reports.
CSCtc36563	Unable to get the PSIRT report via Proxy server.
CSCtc80794	Sync Archive jobs fail in Multi Homed Servers.
CSCtd25864	For ASR 1000, RME polls old-cisco-chassis-mib instead of entity-mib.
CSCtd26836	For archive jobs, report attachment is not enabled in email.
CSCtd45156	Netconfig schema changes are incorrect after restore.
CSCtd75084	Devices with crypto certificates are reported as Out of Sync.
CSCtd91570	When you remove a device from RME, with the Group Selector set to Device, Sync Archive Job will fail.
CSCte11439	In RME 4.3, Inventory collection fails as the column size of the DB is small.
CSCte15460	RME does not properly manage Catalyst 2960 and 3560 series switches in a clustering environment.

Table 15 **Caveats of RME 4.3 Resolved in CiscoWorks LMS 4.0 (continued)**

Identifier	Headline
CSCte26450	Unable to run RME multi service port report for Cisco 7606-S device
CSCte29339	Vulnerabilities in Cisco Works CWCLI
CSCte39507	RME Inventory Reports SysUpTime does not work as expected.
CSCte49301	The EssentialsDM daemon gets stuck in a Waiting to initialize state
CSCte62503	Unable to fetch recommendations for 2851 routers.
CSCte66765	RME 4.3.1 Inventory Collection fails using SNMPv3 for ASA 5520 with 8.2(1)11 image.
CSCte71764	PSIRT/EoX reports do not work due to problems in Cisco.com.
CSCte95623	CDA and Config Archive jobs fail for IOS-XR devices using SSHv2.
CSCte95636	Inventory collection fails for the IOS-XR device with 3.8.1 image.
CSCte98853	RME cannot archive configs for Nexus 5000 and 7000 devices
CSCtf07528	Syslog messages for Content Service Switches do not appear in syslog reports.
CSCtf29160	SWIM may not be able to upgrade standby supervisors on Catalyst 6500.
CSCtf29219	Contract connection log contains Cisco.com passwords.
CSCtf29843	Device Credential Verification Job does not appear as Failed when TACACS fails
CSCtf48565	Inventory collection always detects the value of the Reboot Config Register.
CSCtf52734	System-defined automated action types can be modified.
CSCtf52734	Syslog automated actions for Config and Inventory Fetch can be modified to change their type to email, script, or URL.
CSCtf70684	Netshow job for `show run	in time-zone` fails with an error even though the command is successfully deployed.
CSCtf82992	IPSLA configuration is not processed properly.
CSCtg26155	Trailing spaces are appended to commands deployed to devices.
CSCtg26179	When deploying a compliance job in RME, sub-interfaces are not removed, despite being configured in a baseline template.
CSCtg31710	RME compliance deploy job sends the reload command to partially successful devices, when it retries to deploy the same compliance deploy job.
CSCtg43962	Configuration management operations such as configuration fetch or Netconfig deployment fail to complete.
CSCtg80662	An error appears when you launch the Inventory Collection Summary.
CSCtg91550	RME 4.3 baseline compliance check may fail.
CSCtg41197	RME Config Archive does not archive the vlan.dat for 2800 ISR routers.
CSCth07889	Netconfig jobs may fail if the commands to be executed include the pipe symbol.
CSCth23945	In RME 4.3.1, Netshow NullPointerException appears for devices with null DeviceID
CSCth45005	RME Change Audit Portlet shows unauthorized devices.

Table 15 *Caveats of RME 4.3 Resolved in CiscoWorks LMS 4.0 (continued)*

Identifier	Headline
CSCth47018	RME 4.3.1 Device Credential Verification Job may get stuck when it tries to login via SSH.
CSCth51901	RME 4.3 Netconfig does not properly process the `eigrp` command on 3750ME
CSCth57243	RME Config Archive fails for Nexus devices.
CSCth81713	Device Credential Verification uses Secondary Credential for SSH Enable test.
CSCth84182	Archived configurations are truncated.
CSCti28672	Migration from previous version may not restore device configurations.

Caveats of CS 3.3 Resolved in CiscoWorks LMS 4.0

Table 16 lists the Caveats of Common Services 3.3 resolved in CiscoWorks LMS 4.0

Table 16 *Caveats of CS 3.3 Resolved in CiscoWorks LMS 4.0*

Identifier	Headline
CSCsw73745	Out of memory error appears during selective backup.
CSCsz45041	During Discovery, the size of the DiscoveryStatusObj file grows bigger.
CSCsz58246	After you run the hostname change script, CiscoWorks home page does not display the new hostname in the browser title, and export of user-defined groups does not work.
CSCtf02783	Difficult to obtain a full thread dump from Java daemons.
CSCtf54872	Enhancement request for the Apache flaw: mod_isapi module unload flaw CVE-2010-0425
CSCtf81943	Device may be affected by an OpenSSL vulnerability (CVE-2010-0740).
CSCti74728	Apache crashes leaving a core dump, and CiscoWorks web interface cannot be accessed.
CSCti59039	LMS 3.2 dbmonitor process may generate a core file.
CSCte66560	LMS 3.2 SSL certificate generation uses MD5, which is considered weak algorithm.
CSCtg76942	CiscoWorks daemons do not properly start, and Tomcat stdout.log contains many exceptions.

Caveats of CM 5.2 Resolved in CiscoWorks LMS 4.0

Table 17 lists the Caveats of Campus Manager 5.2 resolved in CiscoWorks LMS 4.0

Table 17   Caveats of CM 5.2 resolved in CiscoWorks LMS 4.0

Identifier	Headline
CSCsl79490	VLANs in Access points appear inactive in User Tracking Acquisition.
CSCsm96911	In topology, you can view unauthorized devices in VTP domain.
CSCtc31966	User Tracking shows many duplicate IP phones.
CSCtc73048	If there are Access points in the VTP network, an error about VTP Disconnected Domain appears in the Discrepancy Report.
CSCtd35792	Subnet mask field is blank after UT Minor Acquisition.
CSCtd45272	Unable to sort User Tracking reports based on phone numbers.
CSCtd49439	Campus Manager Data Collection does not stop and User Tracking acquisition does not happen.
CSCtd51845	IP Phone report shows duplicates.
CSCte61900	During Data Collection, SNMP Auth fails when querying BRIDGE-MIB based on vlan context.
CSCte65656	UT duplicates phone entries when major acquisition runs more than once.
CSCtf29167	After running a User Tracking Utility query from a Windows client, the Tomcat daemon stops, and CiscoWorks applications can make no further requests until you restart Daemon Manager.
CSCtf04476	Link utilization in Topology View is shown incorrectly in Campus Manager.
CSCtg66941	dot1xEnable will appear false in UT reports even it is true.
CSCtg20882	User Tracking does not start due to the presence of xmlwrite.lock file.
CSCti18910	Data Collection does not complete

Caveats of DFM 3.2 Resolved in CiscoWorks LMS 4.0

Table 18 lists the caveats of DFM 3.2 resolved in CiscoWorks LMS 4.0.

Table 18   Caveats of DFM 3.2 resolved in CiscoWorks LMS 4.0

Identifier	Headline
CSCsx23656	sm_server process does not stop when daemons are stopped.
CSCsu01718	In DFM, devices get stuck at 70% Learning state.
CSCsz30972	LMS5K: Unable to create Notification Groups in a Solaris server with 5000 devices.
CSCsz21918	The entSensorStatus value appears as UNKNOWN for the VSS switch and an invalid alert is generated.
CSCsz81452	Unable to create a Customizable Interface Group based on the Interface Description (Alias).
CSCta03602	DFM does not support all cefcModuleOperStatus states.

Table 18   Caveats of DFM 3.2 resolved in CiscoWorks LMS 4.0 (continued)

Identifier	Headline
CSCta31193	For ASA 5540 Device, CPU Usage may not be available in DDV.
CSCtb77134	The email subject customization feature in Device Fault Manager does not add User-defined fields if the field names are changed from the default user_defined_field_X.
CSCtb87449	DFM generates alerts for administratively down interfaces.
CSCtc18926	DFM generates alerts for Voltage Sensor in ASR devices.
CSCtg29656	DFM does not generate an environment alarm for the Cat4500 platform when the ciscoEnvMonSupplyState is notFunctioning state.
CSCtg43956	Notifications such as email, trap, and syslog messages are not sent.

Caveats of IPM 4.2 Resolved in CiscoWorks LMS 4.0

Table 19 lists the caveats of IPM 4.2 resolved in CiscoWorks LMS 4.0.

Table 19   Caveats of IPM 4.2 resolved in CiscoWorks LMS 4.0

Identifier	Headline
CSCsy74148	Error occurs in ACS while importing collectors with DHCP and AutoIPSLA.
CSCta65974	Sometimes, the adhoc device is not added to IPM.
CSCtb00574	IPM loses all of its data; all devices and collectors must be re-added to the application.
CSCtb58619	Examples and detailed information about input file formats, when importing IPM Collectors, is not available in the IPM documentation.
CSCte16115	IPM Collection status appears as Source not Responding.
CSCth13771	In some cases, System Reports are missing when you upgrade to IPM 4.2.

Caveats of HUM 1.2 in CiscoWorks LMS 4.0

Table 20 lists the caveats of HUM 1.2 resolved in CiscoWorks LMS 4.0.

Table 20   Caveats of HUM 1.2 resolved in CiscoWorks LMS 4.0

Identifier	Headline
CSCtc75340	The following error message appears when you create a poller in HUM: `Cannot communicate with Poller Manager Service. Check whether the UPMProcess is down.`
CSCsx47253	Separate Device Management is not available for HUM.
CSCtb68766	HUM does not create a poller for PIX/ASA CPU utilization.
CSCtc65312	Trap for ciscoEpmHealthNotificationAlarm is improper.
CSCtd78310	In Poller Management, HUM poller shows incorrect interface name when you delete and add interfaces on the managed device.

Table 20   Caveats of HUM 1.2 resolved in CiscoWorks LMS 4.0 (continued)

Identifier	Headline
CSCtf30642	Problems occur while loading the CISCO-VOICE-DIAL-CONTROL-MIB into HUM.
CSCtf94360	When you query a table in a MIB, only a few instances appear, and errors appear in the upm_process.log.
CSCtg91090	Interface utilization polling job stops suddenly, and resumes later. If polling is done for a group of devices, polling stops for the group.
CSCth45032	HUM shows unauthorized devices in the Device Selector of Poller Management.

Product Documentation

Table 21 describes the product documentation that is available.

Table 21   Product Documentation

Document Title	Available Formats
Release Notes for CiscoWorks LAN Management Solution 4.0 (this document)	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/release/notes/lms40rel.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
Context-sensitive online help	Select an option from the navigation tree, then click Help.
Getting Started with CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/user/guide/getting_started/gsug.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
Configuration Management with CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/user/guide/configuration_management/cmug.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
Monitoring and Troubleshooting with CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/user/guide/monitoring_troubleshooting/mntug.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
Inventory Management with CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/user/guide/inventory_mgmt/inventory.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.

Table 21 **Product Documentation**

Document Title	Available Formats
Administration of CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks _lan_management_solution/4.0/user/guide/admin/admin. html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
Technology Work Centers in CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks _lan_management_solution/4.0/user/guide/work_centers/ wc.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
Reports Management with CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks _lan_management_solution/4.0/user/guide/Reports/rptm gt_ug.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
Installing and Migrating to CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks _lan_management_solution/4.0/install/guide/install.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
Navigation Guide for CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks _lan_management_solution/4.0/navigation/guide/nav_gu ide.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
Open Database Schema Support in CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks _lan_management_solution/4.0/database_schema4.0/gui de/dbviews.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.
Supported Devices Table for CiscoWorks LAN Management Solution 4.0	• On Cisco.com at http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks _lan_management_solution/4.0/device_support/table/lms 40sdt.html • PDF version part of CiscoWorks LMS 4.0 Product DVD.

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.

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.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

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

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

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

Original SSLeay License:

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

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

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

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

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

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

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

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

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