Configuration Management with Cisco Prime LAN Management Solution 4.1

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-20718-01

Configuration Management with Cisco Prime LAN Management Solution 4.1

CONTENTS

Preface

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

Cisco Prime LMS 4.1 has a new menu layout that facilitates access to information and to tools required for managing your network.

Cisco Prime LMS 4.1 groups options to the following underlying core functions in this release:

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

This guide provides you with information on the Configuration Management function in Cisco Prime LMS.

This preface lists related documents that support the Configuration Management function, and demonstrates the styles and conventions used in this guide. The preface contains the following sections:

Audience

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

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

Document Conventions

Table 1 describes the conventions followed in the user guide.

Table 1 Conventions Used

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

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

Product Documentation

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

Table 2 describes on the product documentation that is available.

Table 2 Product Documentation

Document Title	Available Formats
Getting Started with Cisco Prime LAN Management Solution 4.1	PDF version part of Cisco Prime LMS 4.1 Product DVD.
Context-sensitive online help	Select an option from the navigation tree, then click Help.
Configuration Management with Cisco Prime LAN Management Solution 4.1 (This document)	PDF version part of Cisco Prime LMS 4.1 Product DVD.
Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1	PDF version part of Cisco Prime LMS 4.1 Product DVD.
Inventory Management with Cisco Prime LAN Management Solution 4.1	PDF version part of Cisco Prime LMS 4.1 Product DVD.
Administration of Cisco Prime LAN Management Solution 4.1	PDF version part of Cisco Prime LMS 4.1 Product DVD.

Table 2 Product Documentation

Document Title	Available Formats
Technology Work Centers in Cisco Prime LAN Management Solution 4.1	PDF version part of Cisco Prime LMS 4.1 Product DVD.
Reports Management with Cisco Prime LAN Management Solution 4.1	PDF version part of Cisco Prime LMS 4.1 Product DVD.

Obtaining Documentation and Submitting a Service Request

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

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

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

Notices

The following acknowledgements pertain to this software license.

OpenSSL/Open SSL Project

LMS includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/), and cryptographic software written by Eric Young (eay@cryptsoft.com), and 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. The license texts are listed below. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

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

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

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

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

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

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

Original SSLeay License:

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

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

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

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

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

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

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

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

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

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

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

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

CHAPTER 1

Overview of Configuration Management

Configuration Management in Cisco Prime LAN Management Solutions (LMS) allows you to manage, deploy, and modify the configuration files used by devices in your network. You can run tools that can compare configuration files and perform software image management tasks.

Configuration Dashboard in LMS provides information such as, date of last configuration change, status of the configuration jobs, summary of inventory configuration protocol, Hardware and Software summary.

You can create configuration jobs and also manage configuration archive settings. You can define baseline configuration templates and determine the devices that are non-compliant in your network.

You can perform VLANs configurations and Virtual Switching System (VSS) conversions.

This chapter provides information on the organization of the Configuration Management user guide, and an overview of Configuration Management tasks.

It explains:

What's New in LMS 4.1?

This section contains the following new features of the Configuration Management module of LMS:

Configuration Center

Configuration Center (**Configuration > Configuration Center**) is a launch point for all types of device or feature configurations supported in LMS.

The links to the device or feature configurations are classified under configurations related to:

- Technologies and Services
- Validated Designs
- Configuration Tools

For more information, see Configuration Center.

Enhancements in Template Center

- Grouping of templates

  The templates in Template Center are grouped into:

  – Custom Templates—Lists all the user-defined templates assigned to the current user.

  – Cisco Best Practises Templates—Lists all the system-defined templates

- Reference for each template

  You can add a link or specify a file that provides additional information about the template. The reference files can have the following extensions: html, txt, csv, pdf, doc, docx, xls, xlsx, and have to be stored in the location:
  NMSROOT\htdocs\config-templates-help (On Windows) and
  NMSROOT/htdocs/config-templates-help (On Solaris and Soft Appliance).

- Tag templates

  You can specify tags for your template. These tags can be used as filters for the templates. You can specify multiple tags for a single template, each tag should be comma separated.

- Filter templates

  Template Center has two types of filters:

  – Quick Filter

  – Advanced Filter

  These filters provide various options for you to query and filter the required templates.

- Multi-line Command Support

  You can enter multi-line commands like, banner and crypto certificate commands, as a part of the templates in Template Center. The multi-line commands must be within the tag <MLTCMD> and </MLTCMD>. The commands within the MLTCMD tags are considered as a single command and will be downloaded as a single command onto the device

  These tags are case-sensitive and you must enter them only in uppercase. You cannot start this tag with a space. You can have a blank line within a multi-line command.

For more information, see Managing and Deploying Templates.

Organization

The Configuration Management user guide is organized as follows:

Table 1-1 Configuration Management User Guide

Chapter	Description
Chapter 1, "Overview of Configuration Management" (This chapter)	Provides information on the organization of Configuration Management with Cisco Prime LMS user guide and an overview of the tasks in Configuration Management functionality.
Chapter 2, "About Configuration Dashboard"	Describes the Configuration Dashboard portlets in LMS.
Chapter 3, "Managing and Deploying Templates"	Describes how to manage configuration templates and deploy them on devices.
Chapter 4, "Making and Deploying Configuration Changes Using NetConfig"	Describes how to use the NetConfig feature in Configuration Management. NetConfig allows you to make configuration changes to your managed network devices whose configurations are archived in the Configuration Archive.
Chapter 5, "Archiving Configurations and Managing them using Configuration Archive"	Describes how to use the Configuration Management feature. Configuration Management gives you easy access to the configuration files for all devices or Cisco IOS-based Catalyst switches, Content Service Switches, Content Engines, and Cisco routers in the LMS inventory.
Chapter 6, "Using Baseline Templates to Check Configuration Compliance"	Describes how to use Compliance management task to create, deploy, manage baseline templates. It also describes how to check for configuration compliance.
Chapter 7, "Editing and Deploying Configurations Using Config Editor"	Describes how to use the Config Editor task. Config Editor allows you to edit a configuration file that exists in the configuration archive.
Chapter 8, "Managing Software Images Using Software Management"	Describes how to use the Software Image Management tool in LMS. To ensure rapid, reliable software upgrades, Software Management automates many steps associated with upgrade planning, scheduling, downloading, and monitoring.
Chapter 9, "Virtual Switching System Support"	Describes how to convert two standalone switches into a Virtual Switching System. It also describes how to convert a Virtual Switching System back to standalone switches.
Chapter 10, "Configuring VLAN"	Describes how to configure and manage a Virtual Local Area Network (VLAN) in your network. It also describes how to configure and manage a Private VLAN (PVLAN), Trunk, and also assign ports to VLANs.

Table 1-1 Configuration Management User Guide

Chapter	Description
Chapter 11, "Configuring Virtual Routing and Forwarding (VRF)"	Describes how to perform end-to-end VRF configurations in an enterprise network using LMS.
Chapter 12, "Viewing Topology Services"	Describes how to view and monitor your network including the links and the ports of each link using Topology Services in LMS.
Chapter 13, "CLI Utilities"	Describes how to use the CiscoWorks Command Line (CWCLI) utilities in LMS.

Configuration Management Tasks

This section provides an overview of the Configuration Management tasks supported in LMS. The information is organized as follows:

Configuration Tasks	Menu Navigation Path	Description
Dashboard		
Configuration	Configuration > Dashboard: Configuration	You can view and configure the following configuration dashboard portlets: • Best Practices Deviation • Discrepancies • Job Information Status • Device Change Audit • Inventory Config Protocol Summary • Hardware Summary • Job Approval • Software Summary • Syslog Alerts
Compliance		
Compliance Templates	Configuration > Compliance: Compliance Templates	You can perform the following compliance tasks: • Manage Baseline templates • Run compliance check • Deploy Baseline templates • Run compliance check and deploy jobs
Out-of-Sync Summary	Configuration > Compliance: Out-of-Sync Summary	You can generate an Out-of-Sync report for the group of devices for which running configurations are not synchronized with the startup configuration.

Configuration Tasks	Menu Navigation Path	Description
Job Browsers		
Compliance	Configuration > Job Browsers: Compliance	You can view the compliance check and deploy job status.
Configuration Archive	Configuration > Job Browsers: Configuration Archive	You can manage archive management jobs.
Template Center	Configuration > Job Browsers: Template Center	You can browse the template deployment jobs registered on the system. Using the Template Center, you can manage template jobs. That is, you can stop, delete, refresh, or filter jobs using this job browser. You can also view the template job details such as work order, device details, and job summary.
NetConfig	Configuration > Job Browsers: NetConfig	Using the c Job Browser, you can manage NetConfig jobs. That is, you can edit, stop, delete, or filter jobs using this job browser.
Software Image Management	Configuration > Job Browsers: Software Image Management	You can view all your scheduled Software Management jobs. You can edit, stop, delete the jobs using the Software Image Management Job Browser.
Config Editor	Configuration > Job Browsers: Config Editor	You can manage configuration editor jobs.
Job Approval	Configuration > Job Browsers: Job Approval	You can approve configuration jobs.
Tools		
Template Center	Configuration > Tools: Template Center	Template Center in LMS provides you with a list of system-defined templates. These templates contain configuration commands that can be deployed on the devices in your network. You can perform the following tasks from Template Center: • Deploying Templates • Managing Templates • Importing Templates • Assigning Template to users • Viewing and Managing Template Center Jobs
NetConfig	Configuration > Tools: NetConfig	You can perform the following NetConfig tasks: • Deploying NetConfig jobs • Assigning Tasks to users • User Defined Tasks

Configuration Tasks	Menu Navigation Path	Description
Config Editor	Configuration > Tools: Config Editor	You can open a configuration file, edit it, save it in a private location or in public location using the following tasks: • Open and edit config files • Save config files as private • Save config files as public
Software Image Management	Configuration > Tools: Software Image Management	You can perform the following Software Image Management tasks: • Patch Distribution • Software Distribution • Software Repository • Repository Synchronization • Upgrade Analysis • Software Management Jobs
Workflows		
VLAN	Configuration > Workflows: VLAN	You perform the following VLAN tasks: • Configure VLAN • Delete VLAN • Create Private VLAN • Delete Private VLAN • Configure Port Assignment • Configure Promiscuous Ports • Create Trunk • Modify Trunk Attributes
VRF-lite	Configuration > Workflows: VRF-lite	You can perform the following Virtual Routing and Forwarding (VRF) tasks: • Create VRF • Edit VRF • Extend VRF • Delete VRF • Edge VLAN Configuration
Virtual Switching System	Configuration > Workflows: Virtual Switching System	You can convert two standalone switches into a Virtual Switching System or convert Virtual Switching System back to standalone switches.
Configuration Center	Configuration > Configuration Center	You can view all the launch points for all types of device or feature configurations supported in LMS.

Configuration Tasks	Menu Navigation Path	Description
Configuration Archive		
Summary	Configuration > Configuration Archive: Summary	You can view the configuration archival status and summary.
Views	Configuration > Configuration Archive: Views	You can search archives using version tree and version summary. Views lists the following links: • Custom Queries • Search Archive • Version Summary • Version Tree
Synchronization	Configuration > Configuration Archive: Synchronization	You can schedule a job to update the configuration archive for selected group of devices.
Compare Configs	Configuration > Configuration Archive: Compare Configs	You can compare the following configurations: • Startup vs Running • Running vs Latest Archived • Two Versions of the Same Device • Two Versions of Different Devices • Base Config vs Latest Version of Multiple Devices
Label Configs	Configuration > Configuration Archive: Label Configs	A label is a name given to a group of customized selection of configuration files. You can select configuration files from different devices, group and label them.
Protocol Usage Summary	Configuration > Configuration Archive: Protocol Usage Summary	You can view the configuration protocol usage details for successful configuration fetches.
Topology		
Topology Services	Configuration > Topology	You can launch Topology Services to view and monitor your network.

Configuration Center

Configuration Center is a launch point for all types of device or feature configurations supported in LMS.

The various device or feature configurations supported in LMS are

Configuration	Description
Technologies and Services	
Auto Smartport	Auto Smartports macros dynamically configure switch ports based on the device type detected on the port. You can • Assess Auto Smartports readiness of the network. • Upgrade IOS, wherever required, to make the device ASP capable. • Deploy Auto Smartports templates on selected devices. • Add or edit macros, system-defined, user-defined, or remote macro, associated to an event. • Enable or disable Auto Smartports on selected interfaces of the selected devices. • Modify or disable Auto Smartports configuration on ASP enabled devices.
Credential	You can • Configure or change enable or secret password to enter in enable mode on devices. • Configure local username and password authentication on devices. • Configure SSH. • Add, remove, and edit Telnet passwords.
EEM	You can configure Embedded Event Manager (EEM) scripts or applets, and configure EEM Environmental Variables on the devices. You can • Configure EEM scripts or applets on selected devices. • Configure the EEM policy. • Register or unregister a script or applet. • Configure EEM environmental variables that are used by the TCL script.
EnergyWise	You can measure, monitor, and manage the way your devices consume energy. You can • Assess EnergyWise readiness of the network. • Upgrade IOS, wherever required, to make the device EnergyWise capable. • Define EnergyWise domains. • Associate devices to the EnergyWise domain. • Define Endpoint group and configuring EnergyWise policies.

Configuration	Description
Gold	You can configure Boot Level Diagnositc tests and configure GOLD Monitoring tests on devices. You can • Configure Boot Level diagnositc tests. • Configure GOLD monitoring tests. • Configure Health Monitoring diagnostics. • Enable or disable Health Monitoring diagnostics test. • Configure Health Monitoring interval.
Identity	Identity offers authentication, access control, and user policies to secure network resources and connectivity. You can • Assess Identity readiness of the network. • Upgrade IOS, wherever required, to make the device Identity capable. • Configure RADIUS settings. • Configure security modes, authentication profile, and host mode. • Configure MACsec on capable devices.
MACsec	You can configure MACsec to provide secure, encrypted communication on wired LANs. You can use this template to configure: • Security policy to be applied to the session after the supplicant passes 802.1x authentication. • Authentication Failure Policy. • MKA policy.
Performance Monitoring	You can configure the following for endpoints like Cisco Unified Video Advantage (CUVA), Cisco TelePresence Movi, Tandberg, and Webex Servers: • Configure a flow record to specify the fields you want to monitor. • Configure a policy to include one or more classes. • Reaction ID, jitter and threshold of lost packets. You can configure a flow record and specify how the collected data is aggregated and presented.
PfR	Performance Routing provides best path optimization and load balancing of traffic over the WAN and to the Internet for enterprise networks with multiple paths. You can: • Configure traffic classes for performance routing. • Configure performance metrics of these individual traffic classes. • Control the traffic by applying suitable traffic class and link policies.

Configuration	Description
Port Macros	You can configure Auto Smartport macros on devices. You can • Enable or disable Auto Smartport at device level. • Apply or remove Auto Smartport policy definitions.
QoS	This template provides QoS macros to switch ports upon detection of a Medianet endpoint. You can: • Select specific network traffic. • Prioritize it according to its relative importance. • Use QoS macros to provide preferential treatment of traffic in your network.
RSVP	Resource Reservation Protocol (RSVP) signals the QoS needs of an application's traffic, along the devices, in the end-to-end path through the network. You can configure • User or application that requires an RSVP request. • Bandwidth that has to be reserved. • Admission policy that the devices use to admit the RSVP message.
SCH	You can use this template to enable Smart Call Home on MDS, Nexus, IOS and ASA platforms.
SGA	You can propagate the Security Group Tags (SGT) across network devices that do not have hardware support for Cisco TrustSec. You can use this template to configure: • Default SGT Exchange Protocol (SXP) password. • SXP address connection. • Default SXP source IP address.
Smart Install	Smart Install is a configuration and image management feature that provides zero-touch deployment for new devices. You can: • Assess the readiness of your network for Smart Install capable directors. • Upgrade IOS, wherever required, to make the device Smart Install capable. • Discover and enable Smart Install on Smart Install capable directors. • Manage configuration files and images of clients in the Smart Install director. • Configure DHCP settings for Smart Install.
SNMP	You can configure SNMP community strings, SNMP security feature, and SNMP traps on devices.

Configuration	Description
TACACS	You can configure: • TACACS authentication • TACACS+ authentication • RADIUS on devices
Video Conferencing	You can use this template to configure different video endpoints for video conferences. You can configure three types of video profiles: • Homogeneous Video Conference • Heterogeneous Video Conference • Guaranteed Audio Conference
Video Transcoding	You can use this template to configure video transcoding when the bit rate, frame rate, resolution, or codec is different between two endpoints.
VLAN	You can configure and manage VLAN, Private VLAN (PVLAN), Trunk, and also assign ports to VLANs.
VRF-Lite	You can select Layer 2 or Layer 3 devices and configure VRF on the selected devices. You can • Select the Layer 2 or Layer 3 devices from the Distribution Layer or the Core Layer. • Configure VRF on the selected devices. • Configure details of the VRF like: VRF Name, Route Distinguisher, and description of VRF. • Map an interface to a VRF. • Configure the routing protocol to the selected devices on which VRF is configured.
VSS	You can convert VSS-capable standalone switches to a Virtual Switching System. You can • Select devices for VSS configuration • Perform hardware compatibility checks on the devices • Perform software compatibility checks on the devices and generate compliance report • Define configuration parameters • Deploy commands on the devices to enable VSS mode
Validated Designs	
Access Switch Configuration	You can use this template to configure QoS, rate limiting, ACLs, OSPF for routed access, and IPv6 on Access switches.
Cisco Smart Business Architecture	This template provides resilience, QoS, security, and, scalability for Cisco Smart Business Architecture (SBA) networks.

Configuration	Description
Small Branch Configuration	You can use this template to configure security features like GETVPN, DMVPN, Firewall, IPS and unified communications.
Configuration Tools	
NetConfig Templates	You can configure: • General Settings NetConfig provides system-defined configuration tasks. You can create configuration commands by using these tasks All System-defined tasks are categorized into various task groups in the Tasks Selector. • User-defined tasks You can create user-defined tasks and add one or more templates to each task. The templates contain configuration commands and rollback commands. You can enter the configuration commands either by typing them or by importing them from a file. The template is associated with the MDF categories of devices, for which these templates will be applicable.
Template Center	You can deploy system-defined templates and user-defined templates on devices in your network. You can configure the following types of templates: • Custom Templates—Lists all the user-defined templates assigned to the current user. • Cisco Best Practises Templates—Lists all the system-defined templates

CHAPTER 2

About Configuration Dashboard

This chapter provides information on the Configuration dashboard in LMS.

Configuration dashboard in LMS provides provides information such as, the date of last configuration change, status of the configuration jobs, summary of configuration protocol, Hardware and Software summary.

The Configuration dashboard shows the following list of portlets:

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

Best Practices Deviation

You can view the deviation type and the number of deviations using the Best Practices Deviation portlet.

The Best Practices Deviation portlet helps you to view deviations from normal or recommended practices in a network and provides information on each of the Best Practice deviations reported in LMS. These deviations do not have a serious impact on the functioning of the network.

This portlet gives a description of the Best Practice Deviation. It includes the impact, if any, that the deviation has on the network, and ways to resolve the deviation.

Table 2-1 lists Best Practices Deviation portlet details.

Table 2-1 Best Practices Deviation

Field	Description
Type	Brief description of the deviation from the Best Practice.
Count	Number of deviations. Click the number corresponding to the deviation to navigate to the Unacknowledged Best Practices Deviation Reports. This page displays details such as the type, summary, first found and remarks.

You can click the portlet name in the title bar to navigate directly to the Report Generator page. Select **Best Practices Deviations** from the Select a Report drop-down list to navigate to the Best Practices Deviations page.

Discrepancies

In the Discrepancies portlet, you can view the type and count of discrepancies, such as network inconsistencies and anomalies or misconfigurations in the discovered network.

The Discrepancy portlet gives a description of the discrepancy, the impact it has on the network, and ways to resolve it.

LMS provides reports on discrepancies in the discovered network, enabling identification of configuration errors such as link-speed mismatches on either end of a connection. Discrepancies are computed at the end of each data collection schedule.

Table 2-2 lists the Discrepancies portlet details.

Table 2-2 Discrepancy

Field	Description
Type	Type of the discrepancy such as network inconsistencies, anomalies or misconfigurations in the network. The available types are: • Port is in Error Disabled State—Count of switch ports in the discovered network have a status of errDisable. • VTP Disconnected Domain—Count of devices that are part of the same VTP domain have different VTP configuration revision numbers. • Link Duplex Mismatch—Count of discrepancies when there is a duplex mismatch between links. • Devices with duplicate SysName—Count of discrepancies when LMS discovers two devices with the same SysName • Trunk VLANs Mismatch—Count of discrepancies when the list of active or allowed VLANs between the two ends of a trunk do not match.
Count	Number of deviations. Click the number corresponding to the deviation to navigate to the Unacknowledged Discrepancy Report in the application.

You can click the portlet name in the title bar to navigate directly to the Report Generator page. Select **Discrepancies** from the Select a Report drop-down list to navigate to the Network Discrepancy page.

Job Information Status

In the Job Information Status portlet, you can view the status of up to 20 jobs of the installed applications. You can click the portlet name in the title bar of the portlet to navigate to the Job Browser page.

Table 2-3 lists Job Information Status portlet details.

Table 2-3 Job Information Status Details

Field	Description
Job ID	Unique ID assigned to the job by the system, when the job is created. The Job IDs are displayed in *ID.No.of.Instances* format in periodic jobs. For example, the Job ID 1002.11 indicates that this is the eleventh instance of the job whose ID is 1002. When you click the Job ID, the job details, if available, are displayed.
Job Type	Type of the job. For example, Inventory Collection, SyslogDefaultPurge, and Net Config Job.

Table 2-3 Job Information Status Details

Field	Description
Status	Status of the scheduled jobs that are completed. The Job states include Succeeded, Failed, Crashed, Cancelled, and Rejected. The status of the succeeded jobs are displayed in green and the Failed, Crashed, Cancelled, and Rejected jobs are displayed in red.
Job Description	Description of the job provided by the job creator. It can contain alphanumeric characters.
Owner	Name of the user who created the job.
Scheduled At	Date and time when the job is scheduled to run.

Device Change Audit

In the Device Change Audit portlet, you can view the changes in the inventory and configuration information for all the devices after every Inventory or Configuration Collection.

However, the VLAN config change details will not be displayed.

The changes in the exception period are displayed in red.

Table 2-4 lists the Device Change Audit portlet details.

Table 2-4 Device Change Audit Details

Field	Description
Device Name	Device name as entered in the Device and Credential Repository. Click or hover the mouse over the device name to view device details.
User Name	Name of the user who performed the change. This is the name entered when the user logged in. It can be the name under which the LMS application is running, or the name using which the change was performed on the device. The User Name field may not always reflect the user name. The User Name is reflected only when: • Config change was performed using LMS • Config change was performed outside LMS, and the network has username based on AAA security model wherein authentication is performed by a AAA server (such as TACACS/RADIUS or local server)
Creation Time	Date and the time at which the application communicated the network change or when Change Audit saw the change record.
Message	Brief summary of the changes in the network change. You can click the Message link to navigate to the 24-hour Inventory Change Report details page.

You can click the portlet name in the title bar to navigate directly to the Report Generator page.

To configure the Device Change Audit portlet:

Step 1 Move the mouse over the title bar of the Device Change Audit portlet to view the icons.

Step 2 Click the Configuration icon. You can:

- Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed Refresh time.
- Select the Only Exception Period Report checkbox to view any of the special or extraordinary period report.

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

Config Protocol Summary

In Config Protocol Summary portlet, you can view the configuration protocol usage details for successful configuration fetches.

Table 2-5 lists the Config Protocol Summary details.

Table 2-5 Config Protocol Summary Details

Field	Description
Protocol	Protocols used by LMS for fetching the configuration.
Config Type	The Configuration types for the various protocols. The available types are: • Running — Count of the successful running configuration fetched for each protocol • Startup — Count of the successful startup configuration fetched for each protocol • VLAN — Count of the successful VLAN configuration fetched for each protocol. This configuration fetch is supported by only Telnet and SSH protocols. Click the Count link to view a detailed report for a protocol and corresponding Config Type. The detailed report shows the list of devices which are accessed using a particular protocol and for which successful Config Fetch has happened. Example: If you click on a Count link, 20, for Telnet protocol and Running config type, a detailed report is generated with the following fields: – Device Name — Display name of each device. – Accessed At — Date and time at which each device was accessed for Config Fetch purpose. – Config Type — Configuration type for each device. – File Type -— Configuration file type for each device. – This detailed report shows only the devices for which Telnet has successfully fetched configurations. You can use the export icon to export the list of devices from this detailed report to the device selector.

Table 2-5 Config Protocol Summary Details (continued)

Field	Description
Config NeverCollected	The count of devices for which configuration fetch has never happened. Click the Count link to launch the Configuration Never Collected Device page.
Edit Protocol Order	Click this button, if you want to change the transport protocol order.

Hardware Summary

In the Hardware Summary portlet, you can view a pie graph that displays the distribution of all managed Cisco devices in the inventory.

The portlet has the following view options:

- View as Grid—Shows the information in a table format.
- View as Chart—Shows the information in a pie-chart format.

Table 2-6 lists Hardware Summary portlet details.

Table 2-6 Hardware Summary

Fields	Description
Network Management	Percentage of network management used.
DSL and Long Reach Ethernet	Percentage of Ethernet used.
Security and VPN	Percentage of security and VPN used.
Switches and Hubs	Percentage of switches and hubs used.
Routers	Percentage of routers used.
Count	Count of the devices. For instance, you can click the number corresponding to Switches and Hubs to navigate to the Hardware Report details page.

The graph plots the percentage count of devices, based on Cisco MetaData Framework (MDF) categorization of devices.

Each section represents the device category, the device count and percentage of total devices. The graph displays the device category and the percentage of distribution in the network.

You can click the portlet name in the title bar to navigate directly to the Report Generator page.

Job Approval

In Job Approval portlet, you can view the list of all jobs.

Table 2-7 lists Job Approval portlet details.

Table 2-7 Job Approval Details

Field	Description
Job ID	ID of the job that has been given for approval. The unique number assigned to the job. For periodic jobs such as Daily, Weekly, and so on, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3, indicates that this is the third instance of the job ID 1001. Click the Job ID hyperlink to view the job details.
Job Description	Description of the job.
Job Schedule	Date and time for which the job has been scheduled.

The Job Approval portlet allows you to approve or reject a job for which you are an approver. A job will run only if it is approved. If the job is not approved by its scheduled runtime, or if an approver rejects it, the job is moved to its rejected state and will not run.

For periodic jobs, only one instance of the job needs to be approved. If one instance is approved, all other instances are also considered as approved.

You are notified by e-mail, when a job that has to be approved by you is created.

This portlet enforces the approval process by sending job requests through e-mail to people on the approver list.

You can click the portlet name in the title bar to navigate directly to the Jobs Pending Approval details page in LMS.

In the Job Approval portlet, you can view the list of Job details.

You can configure the Job Approval portlet to set the number of records to be displayed in the portlet and refresh time both manually and automatically.

To configure the Job Approval portlet:

Step 1 Move the mouse over the title bar of the Job Approval portlet to view the icons.

Step 2 Click the Configuration icon.

Step 3 You can:

- Select the minute and hour from the Refresh Every drop-down list to change the refresh time. The items in the portlet get refreshed at the changed Refresh time.
- Select the number of records to be displayed in the portlet from the Show Last Records drop-down list.

Step 4 Click **Save** to view the portlet with the configured settings.

Software Summary

In the Software Summary portlet, you can view the software version information and count for selected devices such as Cisco Interfaces and Modules, Switches and Hubs, Universal Gateways and Access Servers, and Routers.

Table 2-8 lists the Software Summary portlet details.

Table 2-8 Software Summary

Fields	Description
Device Categories	Categories of devices used in the application.
Software Version	Software version of the device categories.
Count	Number of devices. For instance, you can click on the number corresponding to Switches and Hubs to navigate to the Software Report details page.

You can click the portlet name in the title bar to navigate directly to the Report Generator page.

To configure the Software Summary portlet:

Step 1 Move the mouse over the title bar of the Software Summary portlet to view the icons.

Step 2 Click the Configuration icon.

You can:

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

  The items in the portlet get refreshed at the changed Refresh time.
- Select the number of rows to be displayed in the portlet from the No.of Rows to be Displayed drop-down list.

Step 3 Click **Save** to view the portlet with the configured settings.

Syslog Alerts

The Syslog Alerts portlet displays the 24-hour Syslog event distribution as a a pie chart. It also displays the total number of Syslog counts.

The portlet displays the top 10 syslog summary reports.

The portlet has the following view options:

- View as Grid—Shows the information in a table format.
- View as Chart—Shows the information in a pie-chart format.

To configure the Syslog Summary portlet:

Step 1 Move the mouse over the title bar of the Syslog Summary portlet

Step 2 Click the configuration icon.

You can:

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

  The items in the portlet get refreshed at the changed refresh time.
- Select the number of rows to be displayed in the portlet from the No.of Rows to be Displayed drop-down list.
- Select the Show graph checkbox.

Step 3 Click **Save** to view the portlet with the configured settings.

CHAPTER 3

Managing and Deploying Templates

This chapter guides you to manage and deploy configuration templates in LMS.

It explains:

- Accessing Template Center
- Deploying Templates
- Managing Templates
- Importing Templates
- Assigning Templates to Users
- Understanding the Template Center Jobs Browser

Accessing Template Center

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

You can make customized versions of these system-defined templates, by exporting them, changing CLI's/parameters in template XML according to needs, and importing it back after changing the template name. You can also import templates from a client machine and these templates are stored as user-defined templates in LMS.

It is highly recommended to the user to understand the commands in the template and use it according to their network requirements and other configurations already done/to be done.

To access Template Center, go to **Configuration** > **Tools** > **Template Center**.

Table 3-1 describes a list of system-defined templates shipped into LMS 4.1.

Table 3-1 System-defined Templates

Template	Description
DMP Location Configuration	This template configures location information on access ports connected to Digital Media Player. This is a port-based template.
Guaranteed Audio	This Template offers voice services with point-to-point guarantees in an MPLS network. It also offers predictable packet delivery characteristics at various network conditions and loads. When you configure this profile, the system attempts to display video for all participants; however, it does not guarantee that the video of all participants is displayed. For those participants whose video is not displayed, participants are downgraded to audio-only and the profile guarantees preservation of the audio portion of the call.
Heterogeneous Video Conference	This template allows the participants to use different video formats. You can configure different frame rates, bit rates, codecs, or resolutions, and you have the flexibility to choose what profiles to configure, depending on the nature of the participants.
Homogeneous Video Conference	This template allows all the participants in the conference to use the same video format. You must configure the same bit rate, frame rate, codec, resolution, and so on . Only one codec, resolution, and bit rate is configured. All other participants are forced to negotiate to match this profile to join the video conference. If negotiation fails, they fall back to audio-only participants.
Identity - Change of Authorization	This template provides a mechanism for changing the attributes of a session after authentication. When a change in authentication, authorization, and accounting (AAA) policy occurs for a user or user group, administrators can send the RADIUS CoA packets from the AAA server, such as the Cisco Secure Access Control Server (ACS), to re-initialize authentication and apply the new policies. In LMS, you can use this CoA template to generate the configuration commands that can be deployed on devices in your network device to enable Change of Authorization on the device.
IPVSC Location Configuration	This template configures location information on access ports connected to IP Video Surveillance Camera. This is a port-based template.
L2 Access Edge Interface Configuration	This template focuses on Ethernet access interface. It provides Cisco best practice for interface configuration that includes Port security, dhcp snooping, IP Source guard (IPSG), Dynamic ARP Inspection (DAI) and Quality of Service (QoS). This template requires global configuration for IPSG, DAI, , and DHCP snooping.
Location Configuration	This template configures location information on access ports connected to any endpoint. This is a port-based template.

Table 3-1 System-defined Templates

Template	Description
MACsec	This template allows you to enable MACsec to provide secure, encrypted communication on wired LANs. MACsec allows unauthorized LAN connections to be identified and excluded from communication within the network. MACsec defines a security infrastructure to provide data confidentiality and data integrity. MACsec can mitigate attacks on Layer 2 protocols and works with any type of traffic carried over Ethernet links. You can use this template to configure: • Security policy to be applied to the session after the supplicant passes 802.1x authentication. • Authentication Failure Policy. • MKA policy. Guidelines for this template: • Select any value from the Authentication Failure Policy drop-down list, only if Static Link Policy is Always Secure Sessions. For other values of Static Link Policy, select No Change as the Authentication Failure Policy. • Enter a value for VLAN To Be Used only if Authentication Failure Policy is Authorize into a VLAN. • Enter a Name of the other MKA Policy only if MKA Policy is Other Policy. **Note** If you do not adhere to these guidelines, wrong commands can get deployed.

Table 3-1 System-defined Templates

Template	Description

Performance Monitoring	You can configure the following for endpoints like Cisco Unified Video Advantage (CUVA), Cisco TelePresence Movi, Tandberg, Webex Servers, and voice data on all endpoints:
	• A flow record to specify the key and non-key fields you want to monitor.
	• A flow monitor that includes the flow record and flow exporter.
	• A class to specify the filtering criteria.
	• A policy to include one or more classes.
	• One or more performance-monitor type flow monitors.
	• Reaction ID, jitter and threshold of lost packets.
	Before you deploy any Performance Monitoring template on a router, you must apply the license command on the router devices.
	To apply the license in a router:
	1. Go to config mode.
	2. Enter the following commands:
	`license boot module <device series> technology-package datak9`
	`wr mem`
	3. Reboot the router.

Performance Monitoring-CUVA	This template allows you to configure Performance Monitor on Cisco Unified Video Advantage (CUVA). CUVA adds video to your communications experience by providing video telephony functionality to Cisco Unified IP phones.
Performance Monitoring-Movi	This template allows you to configure Performance Monitor on Cisco TelePresence Movi. Cisco TelePresence Movi extends the benefits of face-to-face video collaboration to remote workers.
Performance Monitoring-Tandberg	This template allows you to configure Performance Monitor on all Cisco all Tandberg Endpoints. Tandberg video endpoints work together to provide video users with the full functionality of IP telephony.
Performance Monitoring-Voice	This template allows you to configure Performance Monitor for voice data on all endpoints.
Performance Monitoring-Webex Servers	This template allows you to configure Performance Monitor on Webex Servers.
PFR	This template caters for Performance Routing (PFR) that provides best path optimization and advanced load balancing of traffic over the WAN and to the Internet for enterprise networks with multiple paths. You can • Configure traffic classes for performance routing. • Configure performance metrics of these individual traffic classes. • Control the traffic by applying suitable traffic class and link policies.

Table 3-1 System-defined Templates

Template	Description
QoS	This template provides Quality of Service (QoS) macros to switch ports upon detection of a Medianet endpoint. You can • Select specific network traffic. • Prioritize it according to its relative importance. • Use QoS macros to provide preferential treatment of traffic in your network.
RSVP	Resource Reservation Protocol (RSVP) signals the QoS needs of an application's traffic along the devices, in the end-to-end path through the network. You can configure: • User or application that requires an RSVP request. • Bandwidth that has to be reserved. • Admission policy that the devices uses to admit the RSVP message.
SBA	LMS provides various Smart Business Architecture (SBA) templates to configure resilience, QoS, security, and, scalability for SBA networks, for different types of devices. For more information, see Deploying Templates.
SCH	
SCH on IOS and ASA platforms	This template allows you to configure Smart Call Home (SCH) parameters on IOS and ASA devices.
SCH on MDS platform	This template allows you to configure Smart Call Home parameters on MDS devices. **Note** You can use this template only on MDS devices with NX-OS 4.1(3) or higher software version. SanOS is not supported for the HTTPS transport. In this template, when you enter the Contact Phone Number, it should be in international format and begin with a + sign. You can use hyphens but no spaces in between, for example: • +1-100-100-1000 • +11001001000 • +919840011111 The phone number can have a maximum of 17 characters, including the + sign. LMS validates only the format of the phone number and not the maximum length. If the phone number has more than 17 characters, the command will fail, when you deploy the template on the device.

Table 3-1 System-defined Templates

Template	Description
SCH on Nexus platform	This template allows you to configure Smart Call Home parameters on Nexus devices. **Note** You can use this template only on Nexus devices with NX-OS 4.1(3) or higher software version. SanOS is not supported for the HTTPS transport. In this template, when you enter the Contact Phone Number, it should be in international format and begin with a + sign. You can use hyphens but no spaces in between, for example: • +1-100-100-1000 • +11001001000 • +919840011111 The phone number can have a maximum of 17 characters, including the + sign. LMS validates only the format of the phone number and not the maximum length. If the phone number has more than 17 characters, the command will fail, when you deploy the template on the device.
SGA Access	The Security Group Access (SGA) Access template allows you to enable SXP on the Access devices and allows you to propagate the Security Group Tags (SGT) across network devices that do not have hardware support for Cisco TrustSec. You can use this template to configure: • Default SGT Exchange Protocol (SXP) password. • SXP address connection. • Default SXP source IP address.
SGA Core	The Security Group Access (SGA) Access template allows you to enable SXP on the Nexus devices and allows you to propagate the Security Group Tags (SGT) across Nexus devices that do not have hardware support for Cisco TrustSec. You can use this template to configure: • Default SGT Exchange Protocol (SXP) password. • SXP address connection. • Default SXP source IP address.
Small Branch EIGRP DMVPN FaxRelay	This Template caters for services ready small branch. The configuration includes security features like DMVPN (primary and backup), Firewall (Zone based), IPS and unified communications (SRST). The WAN link is T1, encapsulation is Frame Relay. Backup is SHSDL with ATM IMA. **Hardware and Software Pre-requisites** HWIC-1T1/E1, PVDM2-32, AIM-CUE, 128 MB DRAM, 64 MB flash 1800 series with IOS 12.4.(20)T2 K9 and above with advanced enterprise package.

Table 3-1 System-defined Templates

Template	Description
Small Branch EIGRP DMVPN Only	This Template caters for services ready small branch. The configuration includes security features like DMVPN (primary and backup), Firewall (Zone based), IPS. The WAN link is T1, encapsulation is Frame Relay. Backup is SHSDL with ATM IMA. **Hardware and Software Pre-requisites** HWIC-1T, HWIC-2SHDSL, 128 MB DRAM, 64 MB flash 1800 series with IOS 12.4.(15)T7 K9 and above with advanced enterprise package. T100 Crads should be available in the device
Small Branch EIGRP GETVPN FaxPassThrough	This Template caters for services ready small branch. The configuration includes security features like GETVPN (primary) and DMVPN (backup), Firewall (Zone based), IPS and unified communications (CME SIP). The WAN link is T1, encapsulation is PPP. Backup is SHSDL with ATM IMA. **Hardware and Software Pre-requisites** HWIC-1T1/E1, PVDM2-32, AIM-CUE, 128 MB DRAM, 64 MB flash 1800 series with IOS 12.4.(20)T2 K9 and above with advanced enterprise package.
Small Branch OSPF GETVPN FaxPassThrough	This Template caters for services ready small branch. The configuration includes security features like GETVPN (primary) and DMVPN (backup), Firewall (Zone based), IPS and unified communications (SIP SRST). The WAN link is T1, encapsulation is Frame Relay. Backup is SHSDL with ATM IMA. **Hardware and Software Pre-requisites** HWIC-1T1/E1, PVDM2-32, AIM-CUE, 128 MB DRAM, 64 MB flash 1800 series with IOS 12.4.(20)T2 K9 and above with advanced enterprise package.
Video Transcode	The template provides video transcoding services, where video can be converted from one format to another. You can configure video transcoding when the bit rate, frame rate, resolution, or codec is different between two endpoints.

Note The Basic Small Branch Network provides security and network manageability for the small branch, and integrates the various network services into the branch office router. To deploy these templates ensure that device management IP address is configured in Fa 0/0. This template will remove the IP address in all the other interfaces mentioned in the template.

The above note is applicable for templates such as Small Branch EIGRP DMVPN Only, Small Branch OSPF GETVPN FaxPassThrough, Small Branch EIGRP DMVPN FaxRelay and Small Branch EIGRP GETVPN FaxPassThrough.

Supported SBA Templates

LMS provides various SBA templates to configure resilience, QoS, security, and, scalability for Smart Business Architecture networks, for different types of devices. The various SBA templates supported in this release are:

Name of Template	Description
Access Switch Global Configuration	Use this template to configure Virtual LANs, in-band management, DHCP snooping and ARP inspection on the switch.
Distribution Layer Switch Global Configuration	Use this template to configure an in-band management interface, IP unicast routing, and IP multicast routing.
Core Switch Global Configuration	Use this template to configure an in-band management interface, IP unicast routing, IP multicast routing. Use this template to configure an in-band management interface, IP unicast routing, and IP multicast routing.
LAN Switch Universal Configuration	Use this template to configure the features and services that are common across all LAN switches, regardless of the type of platform or role in the network.These are system settings that simplify and secure the management of the solution.
Client Connectivity Configuration	Use this template to configure switch interfaces to support clients and IP phones, port security on the interface, DHCP snooping, and, ARP inspection and BPDU Guard on the interface.
Multicast Source Discovery Protocol (MSDP) for Core Switches	Use this template to enable Multicast Source Discovery Protocol (MSDP) for core switches.
Catalyst 4500 Access Switch Global Configuration	Use this template to configure Virtual LANs, in-band management, DHCP snooping and ARP inspection on the switch.
Catalyst 4500 Distribution Layer Connectivity to Access Layer	Use this template to configure connectivity to access layer switches.
Catalyst 4500 Client Connectivity Configuration	Use this template to configure switch interfaces to support clients and IP phones, port security on the interface, DHCP snooping, ARP inspection and BPDU guard on the interface.
Catalyst 4500 Platform Configuration	This is a platform template that defines macros used in Catalyst 4500 Series templates to apply the platform specific configuration.
Catalyst 4500 and 6500 LAN Switch Universal Configuration	Use this template to configure the features and services that are common across all LAN switches, regardless of the type of platform or role in the network.These are system settings that simplify and secure the management of the solution.
Catalyst 6500 Series switches Platform Configuration	This is a platform template that defines macros used in Catalyst 6500 Series templates to apply the platform specific configuration.
Catalyst 6500 Distribution Layer Switch Global Configuration	Use this template to configure an in-band management interface, IP unicast routing, IP multicast routing.
Catalyst 3750 and 3750X Platform Configuration	This is a platform template that defines macros used in Catalyst 3750 and 3750X series templates to apply the platform specific configuration.
Catalyst 3750G Distribution Layer Switch Global Configuration	Use this template to configure an in-band management interface, IP unicast routing, IP multicast routing.

Name of Template	Description
Catalyst 2960-S and 3750-X Platform Configuration	This is a platform template that defines macros that is used in Catalyst 2960-S and 3750-X series templates to apply the platform specific configuration.
Distribution Layer Aggregation Configuration	Use this template to configure links in the core layer that are configured as point-to-point Layer 3 routed EtherChannels.
Connectivity to WAN Routers and LAN Core	Use this template to configure connectivity to WAN Routers and LAN Core.
Infrastructure Connectivity to Routers for 2960 Switches	Use this template when to connect to a network infrastructure device that does not support LACP like a router.
Catalyst 4500 Infrastructure Connectivity to Switches	Use this template to connect to another switch when LACP is set to active on both sides to ensure a proper EtherChannel is formed.
Catalyst 4500 Infrastructure Connectivity to Routers	Use this template to connect to a network infrastructure device that does not support LACP like a router.
Cat6500 Connectivity to WAN Routers and LAN Core	Use this template to connect to WAN Routers and LAN Core.
Cat6500 Distribution Layer Connectivity to Access Layer	Use this template to configure connectivity to access layer switches.
3750X 3560X Infrastructure Connectivity to Distribution Switch	Use this template to connect to another switch when Link Aggregation Control Protocol (LACP) is set to active on both sides to ensure that a proper EtherChannel is formed.
3750X 3560X Infrastructure Connectivity to WAN Router	Use this template to connect to a network infrastructure device that does not support LACP, like a router
Catalyst 3750 Distribution Layer Connectivity to Access	Use this template to configure connectivity to access layer switches.
Cat 2960S Infrastructure Configuration to Distribution Switches	Use this template to connect to another switch when LACP is set to active on both sides to ensure that a proper EtherChannel is formed.
Catalyst 3560-X Platform Configuration	This is a platform template that defines macros used in Catalyst 3560-X series templates to apply the platform specific configuration.

Deploying Templates

Templates are deployed to devices using Deploy Template job in LMS. You can deploy these templates for devices, ports and modules.

By default, LMS groups the templates as:

- Custom Templates—Lists all the user-defined templates assigned to the current user.
- Cisco Best Practises Templates—Lists all the system-defined templates.

You can use the filter option to group the templates.

In LMS 4.1, click the expandable icon before each template (triangle-shaped) to see the details of each template. For more details, see Template Details.

To deploy a template:

Step 1 Select **Configuration > Tools > Template Center > Deploy**.

The Template Deployment page appears, displaying Template Selector pane.

You can select templates to deploy configurations.

Table 3-2 describes the Template Selector pane.

Table 3-2 Template Selector

Column/Button	Description
Template Name	Shows the name of the system and user-defined templates.
Features	Shows the feature related to the template.
Type	Shows the type of the template (Partial or Complete). • Partial—Supports some of the configurations for the device. • Complete—Supports complete configuration for the device.
Role In Network	Role of the device in the network layer (Edge, Core, Access, Distribution)
Category	Shows the category of the template.
Created By	User who created or imported this template. By default, for all system-defined template it will be System and for SBA templates it will be Cisco.
Scope	Shows the scope of the template for device, port, or module.
Filter (button)	Click **Filter**. Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click **Go** to filter details. The following Filter By options are available: • Template Name—Select **Template Name** and enter the complete name. • Type—Select **Type** and enter the type (partial, complete) • Role In Network—Select **RIN** and enter the RIN (access, distribution, core) • Category—Select **Category** and enter the device category • Created By—Select **Created By** and enter the user name • Scope—Select **Scope** and enter the scope (device, port, module) You can also use wild character (*) along with the search text to filter.

Step 2 Select templates and click **Next**.

You can select:

- One Complete with multiple partial templates
- Multiple partial templates

You cannot select multiple Complete templates.

When you select multiple templates, if conflicting features exists between templates, then the deploy template flow will not proceed and a warning message is shown. See Importing Templates for more information on conflicting features.

The Choose Device Groups pane appears, displaying the Device Selector. Choose the devices, or device groups on which you wish to deploy the templates.

The Device Selector displays devices that are common and applicable to the selected templates.

Note If the devices selected is more than 2000, the progress bar is not shown.

Step 3 Select devices from the Device Selector and click **Next**.

If you are unable to view any devices in the Device Selector, you do not have any supported devices for the template.

If you have selected port-related templates, then Choose Port Groups pane appears, displaying the Port Selector.

If you have selected module-related templates, then Choose Module Groups pane appears, displaying the Device Selector.

Step 4 Select port groups from the Port Group Selector and click **Next**.

If you have selected port-related templates, the Review Port Groups page appears with a list of selected devices and selected ports, from the previous page, associated with each device. Unselect the ports that you want to exclude from the deployment.

Step 5 Click **Next,** the corresponding template pane appears, allowing you to enter the applicable values for the template.

Step 6 Enter the values and click **Next**.

The Adhoc Configuration for Selected Port/Device Groups pane appears, allowing you to enter the configuration commands that will be deployed on the selected devices or ports in addition to the commands in the template. The commands that you enter here will not be validated by LMS.

This is optional.

Step 7 Click **Next**.

The Schedule Deployment pane appears, displaying Scheduler and Job Options details.

Table 3-3 describes the fields and options in the Schedule Deployment pane.

Table 3-3 Schedule Deployment Pane Description

Options/Field	Description
Schedule Options	Specifies the type of schedule for the job: • Immediate—Runs the report immediately. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified date and time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time.
Job Description	Enter a description for the job that you are scheduling. This is a mandatory field. Accepts alphanumeric values and special characters.
E-mail	Enter the e-mail address to which the job sends messages when the job has run. You can enter multiple e-mail addresses separated by comma.
Job Options	The following job options are available: • Copy Startup to Running Config upon failure—If template deployment job fails, the startup configuration of the device is copied to running configuration. • Enable Job Password—Select **Enable Job Password** and enter the Login user name, Login Password and Enable Password details.
Preview CLI (button)	Click **Preview CLI** to open the Configuration Preview pop-up dialog box. You can select the device name from the drop-down list to view the CLI commands that will be deployed on to the device.

Step 8 Enter a Job Description, select the Schedule and Job options and click **Finish**.

A notification message appears along with the Job ID. The newly created job appears in the Template Center Jobs.

Template Details

You can see the following details when you click the expandable icon before each template (triangle-shaped) to see the details of each template:

- Name—Name of the template. For example, Access PortChannel Interface.
- Description—Description of the template. For example, Template for configuring Portchannel Interface on Access Switches.
- Task—Configuration task of the template. For example, Port Configuration.
- Version—Version of the template. For example, 1.0.
- Feature—Features supported for this template.
- Hardware—The hardware platform supported for deploying this template.
- Reference—Displays any reference text for the template. It can be a link for additional information about the template, or a file in the server.
- Tag—Displays the tags that have been specified for the template. You can have multiple tags for a single template. You can use this for filtering the templates using the Advanced Filter.

Managing Templates

LMS allows you to edit, delete, export and view templates.

By default, LMS groups the templates as:

- Custom Templates—Lists all the user-defined templates assigned to the current user.
- Cisco Best Practises Templates—Lists all the system-defined templates.

You can use the filter option to group the templates.

This section details:

- Editing Templates
- Deleting Templates
- Exporting Templates
- Handling Multi-line Commands
- Viewing Template Details

Editing Templates

You can edit the default values of a template (system or user-defined) and save it as user-defined template.

In LMS 4.1, each template has a reference section. In the reference section, you can add a link to provide additional information about the template. The information that you enter in the **Text To Display** text box appears as a link in the expandable pane of the template. When you click the link, it launches the URL or opens the file specified and provides the additional information. You can provide the additional information from a URL or from a file in the server.

The link must start with http://. The reference files can have the following extensions: html, txt, csv, pdf, doc, docx, xls, xlsx, and have to be stored in the location:

- *NMSROOT*\htdocs\config-templates-help (On Windows)
- *NMSROOT*/htdocs/config-templates-help (On Solaris and Soft Appliance)

NMSROOT is the LMS install directory. For Solaris and Soft Appliance, it will be /opt/CSCOpx.

You can also specify tags for your template that can be used as filters for the templates. You can specify multiple tags for a single template, each tag should be comma separated.

To edit a template:

Step 1 Select **Configuration > Tools > Template Center > Manage**.

The Manage Templates page appears, displaying the Template Selector pane.

Table 3-2 describes the Template Selector pane.

Step 2 Select the template that you need to edit and click **Edit**.

The Edit Template page appears.

Step 3 You can edit the Reference link.

Step 4 You can edit the Tag.

Step 5 Edit the default values of the template and click **Save**.

You can create a new template from an existing template (system or user-defined) and click **Save As** to save it as user-defined template.

You can edit a Cisco Best Practices Template and click **Save As** to save the template as a new template.

The Template Management page appears, displaying the Template with edited values.

Deleting Templates

You can use the Delete option to remove an existing template from the Template Selector pane.

Note You cannot delete a system-defined template from the Template Selector pane.

To delete an existing template:

Step 1 Select **Configuration > Tools > Template Center > Manage**.

The Manage Templates page appears, displaying the Template Selector pane.

Table 3-2 describes the Template Selector pane.

Step 2 Select an existing user-defined template from the Template Selector pane.

Step 3 Click **Delete**.

The selected user-defined template is deleted from the Template Selector pane.

Exporting Templates

You can use the Export option to export an existing template to a remote or a client machine. The template exported will be in XML format.

To export an existing template:

Step 1 Select **Configuration > Tools > Template Center > Manage**.

The Manage Templates page appears, displaying the Template Selector pane.

Table 3-2 describes the Template Selector pane.

Step 2 Select an existing template from the Template Selector pane.

Step 3 Click **Export**.

A dialog box appears, prompting you to open or save the template XML file.

Handling Multi-line Commands

In LMS 4.1, you can enter multi-line commands like, banner and crypto certificate commands, as a part of the templates in Template Center. The multi-line commands must be within the tag <MLTCMD> and </MLTCMD>. The commands within the MLTCMD tags are considered as a single command and will be downloaded as a single command onto the device

These tags are case-sensitive and you must enter them only in uppercase. You cannot start this tag with a space. You can have a blank line within a multi-line command.

Example 1

```
<MLTCMD> banner login "Welcome to
Cisco Prime LMS - you are using
Multi-line commands" </MLTCMD>
```

Example 2

```
cmd1<MLTCMD>cmd2
   cmd3
   cmd4
   cmd5</MLTCMD>cmd6
```

Example 2

```
cmd1<MLTCMD>
   cmd2
   cmd3
   cmd4
   cmd5</MLTCMD>cmd6
```

In Example 1 and 2, cmd1,cmd2,cmd3,cmd4,cmd5 and cmd6 are all commands and will be deployed to the device as a single command.

Viewing Template Details

You can use the View Template option to view the details of an existing template from the Template Selector pane.

To view the details of an existing template:

Step 1 Select **Configuration > Tools > Template Center > Manage**.

The Manage Templates page appears, displaying the Template Selector pane.

Table 3-2 describes the Template Selector pane.

Step 2 Select an existing template from the Template Selector pane.

Step 3 Click **View**.

A pop-up window appears, you can view the selected template as XML.

Importing Templates

LMS allows you create a user-defined configuration template by importing:

- Configuration commands from an existing template (.xml file) stored on a client machine (See Importing from XML File)
- A text file generated using Cisco Configuration Professional tool stored on a client machine (See Importing from a Cisco Configuration Professional File)
- A running configuration from a device (See Importing Running Config from Device)

You can also create a new template file (.xml) using the guideline specified in the XML schema. See Config Template XML Schema for information.

You can also download config templates from Cisco.com from the URL: http://www.cisco.com/cisco/software/release.html?mdfid=283434800&flowid=19062&softwareid=283418816&release=Enterprise%20-%20BN%20SBA&relind=AVAILABLE&rellifecycle=&reltype=latest.

Note When you import a template with a name that is already used by another template in LMS, a message appears prompting you to overwrite the template (user-defined) in LMS. System-defined templates cannot be overwritten.

Importing from XML File

To import a template from XML file:

Step 1 Select **Configuration > Tools > Template Center > Import**.

The Import Templates page appears, displaying Choose Import Mode pane.

Step 2 Select **Config Template** from Choose Source Type option.

Step 3 Click **Browse** to select the configuration file (.xml file) stored on a client machine.

Before you import a template, you must ensure that the values of each field do not exceed the respective character limitation. The details are given in the table below.

If the values of each field exceed the character limitation, you will not be able to import the template.

Field	Maximum Number of Characters
Template Name	64
Author	64
Description	1024
Template Version	64
Task	64
Scope	64
Template Type	64
Features	255
Hardware Platform	600

Field	Maximum Number of Characters
PIN	64
Reference Text	100
Reference URL	100
Reference Type	10
Tags	1024

Step 4 Click **Finish**.

A message appears stating that the template has been imported successfully.

Importing from a Cisco Configuration Professional File

To import a template from a Cisco Configuration Professional file:

Step 1 Select **Configuration** > **Tools** > **Template Center** > **Import**.

The Import Templates page appears, displaying Choose Import Mode pane.

Step 2 Select **CCP Config** from Choose Source Type option.

Step 3 Click **Browse** to select the Cisco Configuration Professional file (.txt format) stored on a client machine.

Step 4 Click **Next**.

The View and Edit Configuration pane appears, displaying the configuration commands in the text box.

You can edit these configuration commands. You must ensure that the configuration commands are valid because LMS does not validate these commands.

Step 5 Click **Next**.

The Choose Device Types pane appears.

You need to:

- Choose the image platform for applying the imported configuration from the drop-down list.
- Enter the minimum supported image version for the image platform.
- Choose the device groups for applying the configuration.

Step 6 Click **Next**.

The Choose Conflicting Tags pane appears, displaying the List of Conflicting Features dialog box.

Here, you need to add the list of conflicting features in a file and add it in the Import Template flow. This is optional.

A feature in the template might conflict with a feature of another template. In this case, if you have selected templates that have feature conflicts with each other, then deploy flow will not proceed, and a warning message is shown.

For example,

In the Template Center, you have the following two templates:

- Template A—Deploys Auto Smartport feature and the conflicting feature is CDP
- Template B—Deploys CDP feature

If you have selected both Template A and Template B in the Deploy Template flow, the conflicting feature CDP of Template A with the CDP feature of Template B creates a conflict and this will prevent the Deploy Template job flow to proceed, and a warning message is displayed.

In this case, you have to select templates that do not have feature conflicts with each other and then proceed with the deploy flow.

Table 3-4 describes the fields in the List of Conflicting Features dialog box.

Table 3-4 List of Conflicting Features

Column/Button	Description
Feature	Name of the conflicting feature.
Warning Message	Warning message displayed if the conflicting feature exists
Configuration	Shows the configuration commands of the conflicting feature
Delete (Button)	Delete the conflicting feature file.
Add (Button)	Create a conflicting feature file.
Edit (Button)	Modify an existing conflicting feature file.

Step 7 Click **Next**.

The Enter Template Details pane appears, allowing you to enter the template details described in table.

Table 3-5 describes the fields in Enter Template Details pane.

Table 3-5 Enter Template Details

Field	Description
Template Name	Enter a valid name for the template. Ensure the template name you enter is unique. **Note** When you import a template with a name that is already used by another template in LMS, a message appears prompting you to overwrite the template (user-defined) in LMS. System-defined templates cannot be overwritten. You can enter a maximum of 64 characters.
Description	Provide a description of the template. You can enter a maximum of 1024 characters.
Task	Enter the task description of the template. You can enter a maximum of 64 characters.

Table 3-5 Enter Template Details

Field	Description
Version	Enter the version of the template. You can enter a maximum of 64 characters.
Scope	Choose the scope of the template. For example, device, port, or module.
Feature	Enter the template feature. You can enter a maximum of 255 characters.
Hardware Platform	Enter the applicable hardware platform for the template. You can enter a maximum of 600 characters.
PIN	Choose the PIN (place of the device in the network) for the template. For example, edge.
Image Feature	Enter the image feature for the template.
Type	Choose the type of the template (Complete, Partial)

Step 8 Click **Finish**.

A message appears stating that the template has been created successfully.

Importing Running Config from Device

To import a running config as a template from a device:

Step 1 Select **Configuration** > **Tools** > **Template Center** > **Import**.

The Import Templates page appears, displaying Choose Import Mode pane.

Step 2 Select **Running Config from Device** from Choose Source Type option.

Step 3 Select a device from the Device Selector.

Step 4 Click Next.

The View and Edit Configuration pane appears, displaying the configuration commands in the text box.

You can edit these configuration commands. You must ensure that the configuration commands are valid because LMS does not do any validation on these commands.

Step 5 Click **Next**.

The Choose Device Types pane appears.

You need to:

- Choose the applicable image platform from the drop-down list.
- Enter the minimum supported image version for the image platform.
- Select the applicable device categories from the Device Type Selector.

Step 6 Click **Next**.

The Choose Conflicting Tags pane appears, displaying the List of Conflicting Features dialog box.

Table 3-4 describes the fields in the List of Conflicting Features dialog box.

Step 7 Click **Next**.

The Enter Template Details pane appears, allowing you to enter the template details described in table.

Table 3-5 describes the fields in Enter Template Details pane.

Step 8 Click **Finish**.

A message appears stating that the template has been created successfully.

Assigning Templates to Users

You can assign templates to users with Network Operator and Network Administrator privileges.

A network administrator must assign template access privileges to other users.

Note View the Permission Report (**Reports > System > Users > Permission**) to check whether you have the required privileges to perform this task.

To assign templates to users:

Step 1 Select **Configuration > Tools > Template Center > Assign Template to User**.

The Assign Templates to Users page appears, displaying the Assign Templates dialog box.

Step 2 Enter the username of the user to whom you want to assign the templates.

This should be a valid LMS user.

Step 3 Select the template that you want to allocate to the user from the Available templates list box and click **Add**.

You can select more than one template, by holding down the Shift key while selecting the template.

The selected templates appear in the Selected Templates list box.

To remove assigned templates, select the templates from the Selected Templates list box and click **Remove**.

Step 4 Add all the required Templates to the Selected Templates list box.

Step 5 Click **Assign** to assign the template access privileges to the specified user.

For a specified user, to see the assigned templates, enter the username in the Username field and click **Show Assigned**.

The templates assigned to the user appear in the Selected Templates list box.

Step 6 Click **Report** to generate the User Template Report.

The User Template Report shows the list of users and the templates assigned for each user.

Note By default, all the templates are assigned to admin users. Therefore, the User Template Report will not list the users with Admin privileges.

Understanding the Template Center Jobs Browser

You can browse the template deployment jobs registered on the system. Using the Template Center Jobs, you can manage template jobs. That is, you can stop, delete, refresh, or filter jobs using this job browser. You can also view the template job details such as work order, device details, job summary.

Note View Permission Report (**Reports > System > Users > Permission**) to check whether you have the required privileges to perform this task.

Select either:

Configuration > Tools > Template Center > Jobs.

Or

Configuration > Job Browsers > Template Center

The Template Center Jobs page appears, displaying the List of Template Deployment Jobs pane and Job Details pane for a job.

Table 3-6 describes the List of Template Jobs pane in the Template Center Jobs.

Table 3-6 List of Template Jobs

Column/Button	Description
Job ID	Unique number assigned to a template job when it is created. For periodic jobs such as Daily, Weekly, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the Job ID 1001.
Status	Status of the job: • Successful—When the job is successful. • Failed—When the job has failed. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed amounts to 5. • Stopped—When the job has been stopped. • Running—When the job is in progress. • Waiting—When the job is awaiting approval (if job approval has been enabled). • Rejected—When the job has been rejected (if job approval has been enabled).
Description	Description of the job, entered at the time of job creation.
Owner	User who created the job.
Scheduled at	Date and time at which the job was scheduled.
Completed at	Date and time at which the job was completed.
Schedule Type	Type of job schedule—Immediate, Once, Daily, Weekly, Monthly. For periodic jobs, the subsequent instances will run only after the earlier instance of the job is complete.
Stop (button)	Stop or cancel a running job.
Delete (button)	Deletes the selected job from the Template Center Jobs. You can select more than one job to delete.
Refresh Job (button)	Select a Job and click **Refresh Job**. The Job Details pane gets refreshed showing the latest status of the job.

Table 3-6 List of Template Jobs

Column/Button	Description
Filter (button)	Click **Filter** and select a Filter By criteria from the drop-down list and enter the details in the Equals field. The following Filter By options are available: • Job ID—Select **Job ID** and enter the Job ID number. • Status—Select **Status** and enter the status (Successful, Failed, Cancelled, Running, Waiting, Rejected). • Description—Select **Description** and enter the complete name. • Owner—Select **Owner** and enter the user name. • Scheduled at—Select **Scheduled at** and enter the schedule time details. • Completed at—Select **Completed at** and enter the completed time details. • Schedule Type—Select **Schedule Type** and enter the type (Immediate, Once, Daily, Weekly, Monthly)
Refresh (icon)	Click to refresh the List of Template Jobs table.

Table 3-7 describes the Job Details pane in the Template Center Jobs.

Table 3-7 Template Deployment Job Details

Tab	Description
Work Order	Shows the work order details for the selected job.
General Info	The General Info in the work order displays the following details: • Description—Job description entered at the time of job creation. • Owner—User who created the job. • Schedule Type—Type of job schedule (Immediate, Once, Daily, Weekly, Monthly). • Schedule Time—Time at which the job was scheduled to run. The Schedule Time is applicable for periodic jobs and not for Immediate jobs.
Job Policies	The Job Policies in the work order displays the following details: • E-mail Notification—E-mail notification status (Enabled/Disabled) • E-mail Ids—E-mail IDs registered for e-mail notification • Execution Policy—Job Execution policy as Parallel • Copy Startup to Running Config upon failure—Displays the status (Enabled/Disabled) • Job Password—Login Password for the job. • Job UserName—Login Username for the job.

Table 3-7 Template Deployment Job Details

Tab	Description
Device and Template Details	Shows the following Device and Template details of the job: • Device Template Details • Devices List • Port Template Details • Port Group Details • Module Template Details • Module Details
Device Details	Shows the list of devices added in the Template Deployment job.
Device	Shows the device name.
Status	Status of the device (Success, Failure).
Message Summary	Shows the device status summary.
Show Details	Select the device name and click **Show Details**. A pop-up window appears, displaying the following details for the device: • Device Name—Display name of the device. • Device Status—Status of the device (Success, Failure). • Protocol—Protocol details running on the device. • Summary—Shows the device status summary. • CLI Output—Shows the CLI output.
Filter	Click **Filter**. Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click **Go** to filter details. The following Filter By options are available: • Device—Select **Device** and enter the first few letters or the complete name of the device. • Status—Select **Status** and enter the status (Success, Failure) • Message Summary—Select **Message Summary** and enter the first few letters of the message summary.

Table 3-7 Template Deployment Job Details

Tab	Description
Job Summary	Shows the job summary details for the selected job.
General Info	The General Info in the job summary shows the following details: • Status—Status of the device at the time of job creation. • Start Time—Start time of the job. • End Time—End time of the job.
Job Messages	Shows the following job messages: • Pre-job Execution • Post-job Execution
Device Updates	Shows the following update on the devices in the job: • Successful • Failed • Not Attempted • Pending

CHAPTER 4

Making and Deploying Configuration Changes Using NetConfig

Netconfig is one of the Configuration Management applications that provides you with easy access to the configuration files of all supported devices. It allows you to change the configuration of network devices, provided the configurations are archived. Netconfig automatically updates the archive when it changes the configuration.

The advantages of using Netconfig instead of CLI configuration commands include but are not limited to:

- Scheduling jobs
- Using jobs to run multiple commands on multiple devices
- Using tasks to carry out easy and reliable configuration changes
- Mandating approval before running a job
- Rolling back configuration changes when a job fails

This section contains:

NetConfig Tasks

As a NetConfig user, you can:

- Define and schedule NetConfig jobs

  Use the configuration tasks (system-defined or user-defined) to create the configuration commands that you want to apply to devices.

- Browse and edit NetConfig jobs

  Browse all NetConfig jobs on your system and edit, copy, stop, retry or delete them. For information about a particular job, click the hyperlink of the Job ID in the NetConfig Job Browser.

- Use the command line interface for NetConfig jobs

  Use the cwcli command line interface to create and schedule NetConfig jobs from the command line.

As a NetConfig administrator, you can:

- Create User-defined tasks

  Create your own user-defined tasks containing configuration or rollback commands, and download them to a set of selected devices. You can enter the configuration commands by typing them or by importing them from a file.

  User-defined tasks can be parameterized, that is, they can contain variables that take values from a specified file that resides on the LMS server.

- Assign tasks

  Provide selected network operators the rights to execute configuration tasks. You can assign more than one task to one or more users. By default, only network administrators can use configuration tasks.

- Specify the order of the protocol to deploy the configuration and fetch operations

  Specify the protocol order separately for configuration download and update operations of NetConfig jobs. This enables you to use preferred protocols for downloading and fetching configurations.

  For example, you can use Telnet to download configuration to the device, and TFTP to fetch the configuration, thus improving the overall performance of NetConfig.

- Set default NetConfig job policies

  Each NetConfig job has job properties (including enabling job password) that defines how the job will be executed. You can configure defaults for these properties that will be applied to all future jobs. For each property, you can specify if users can change the default when creating a job.

See Understanding NetConfig User Permissions.

Note You can select the log level settings for the NetConfig application at **Admin > System > Debug Settings > Log Level Settings**.

Preparing to Use NetConfig

This section details the following pre-requisites for using NetConfig:

- Verifying Device Credentials.
- Modifying Device Security
- Verifying Device Prompts
- Configuring Default Job Policies (Optional)
- Assigning Task Access Privileges to Users (Optional)
- Enabling Job Approval (Optional)

Verifying Device Credentials

NetConfig needs access to device credentials to make device configuration changes. The device credentials are available in the Device and Credential repository. Use **Inventory > Device Administration > Add / Import / Manage Devices** to verify if the devices that you want to configure are having the correct credentials.

Modifying Device Security

To configure devices, you must disable security that prohibits NetConfig job from running the commands on the devices. For the list of commands, see *Administration of Cisco Prime LAN Management Solution 4.1*.

Verifying Device Prompts

Table 4-1 describes the CLI prompt formats for NetConfig.

Table 4-1 NetConfig CLI Prompt Formats

Transport Mechanism	Format
Telnet	• For IOS-based devices, Content Engine devices, and Content Service Switch devices – The login prompt must end with a greater-than symbol (>). – The enable prompt must end with a pound sign (#). • For Catalyst devices – The login prompt must end with a greater-than symbol (>). – The enable prompt must end with the text (enable).
SSH	• For IOS-based devices, Content Engine devices, and Content Service Switch devices – The login prompt may end with (>), (#), (:), (%). – The enable prompt must end with a pound sign (#). • For Catalyst devices – The login prompt may end with (>), (#), (:), (%). – The enable prompt must end with the text (enable).

Default prompts use these formats. If the defaults formats have been changed, ensure that the prompts meet these requirements.

Configuring Default Job Policies (Optional)

NetConfig jobs have properties that determine how they run. You can configure the default job policies (Admin > Network > Configuration Job Settings > Config Job Policies) that apply to all NetConfig jobs.

Assigning Task Access Privileges to Users (Optional)

You can assign task access privileges that determine the configuration tasks each user can use to create NetConfig jobs. See Understanding NetConfig User Permissions.

Enabling Job Approval (Optional)

Netconfig jobs require approval before they can run. See the section “Setting Up Job Approval” in *Administration of Cisco Prime LAN Management Solution 4.1*.

Rolling Back Configuration Changes

NetConfig lets you roll back (undo) the configuration changes made to network devices if a job does not gets completed. Rollback commands (the configuration commands that are used to roll back the configuration changes) are created based on how the job was created.

You must configure a NetConfig job to automatically roll back configuration changes, if the job fails to complete.

NetConfig can rollback configurations only if the device configurations are archived in Configuration Archive. See Archiving Configurations and Managing them using Configuration Archive.

This section contains:

- Creating Rollback Commands
- Configuring a Job to Roll Back on Failure

Creating Rollback Commands

For system-defined tasks, the rollback commands are automatically created by the task. For user-defined tasks, you can enter the rollback commands while creating the task.

Configuring a Job to Roll Back on Failure

You can define a job failure policy so that it automatically rolls back configuration changes, if the job fails to run. You can select one of the three rollback options:

- Rollback device and stop—Rolls back the changes on the failed device and stops the job.
- Rollback device and continue—Rolls back the changes on the failed device and continues the job.
- Rollback job on failure—Rolls back the changes on all devices and stops the job.

Understanding NetConfig User Permissions

Access to NetConfig functionality is controlled by permissions. Users having only Help Desk permissions cannot access NetConfig. Other users can access NetConfig, but their access to functionality is controlled.

In the Permission Report (**Reports > System > Users > Permission**) check if you have the required privileges to perform the required NetConfig task.

This section details:

- Job Approval Permissions
- User-defined Tasks Permissions
- Administrator Task Permissions
- Job Editing Permissions

Job Approval Permissions

Users with Approver permissions can approve NetConfig jobs. Jobs must be approved before they are scheduled to run if Job Approval is enabled on the system. See the section “Setting Up Job Approval” in *Administration of Cisco Prime LAN Management Solution 4.1*.

User-defined Tasks Permissions

By default, only users with Network Administrator permissions can create user-defined configuration tasks. For more information, see Creating and Editing User-defined Tasks. A Network Administrator can give other users the required permissions on a task-by-task basis.

Administrator Task Permissions

Network Administrators can perform the tasks listed in the Admin menu.

Administrator tasks are:

- Assigning tasks to users
- Configuring default job properties
- Creating and editing user-defined tasks

For user permissions, see Understanding NetConfig User Permissions.

Job Editing Permissions

After a NetConfig job is created, the owner, or a user with the owner privileges, or a network administrator can:

- Copy a job
- Edit a job
- Retry a job
- Delete a job
- Stop a job while it is running

Using NetConfig

NetConfig allows you to do the following tasks:

- Create and manage NetConfig jobs using the NetConfig job browser. See:
  - Starting a New NetConfig Job
  - Browsing and Editing Jobs Using the NetConfig Job Browser
- Create your own NetConfig tasks and run them on a selected set of devices. See Creating and Editing User-defined Tasks.
- Assign tasks to users. You can assign one or more tasks to one or more users. See Assigning Tasks to Users.

Starting a New NetConfig Job

You can create and schedule:

- Device-based jobs
- Module-based jobs
- Port-based jobs

This section tells you how to:

- Create a NetConfig Job based on Device
- Create a NetConfig Job based on Module or Port

To manage Netconfig jobs using NetConfig job browser, see Browsing and Editing Jobs Using the NetConfig Job Browser.

Ensure that you have set the:

- Transport protocol order for your job using **Admin > Collection Settings > Config > Config Transport Settings**. See *Administration of Cisco Prime LAN Management Solution 4.1*.
- Job and password policy for your job using **Admin > Network > Configuration Job Settings** before starting a new NetConfig job. See *Administration of Cisco Prime LAN Management Solution 4.1*.

Note View the Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Create a NetConfig Job based on Device

To create a new NetConfig job based on Device:

Step 1 Select either:

- **Configuration > Tools > NetConfig > Deploy**

Or

- **Configuration > Job Browsers > NetConfig**

The NetConfig Job Browser appears.

Step 2 Click **Create**.

The Netconfig Job Type page appears, displaying the following job types:

- Device Based
- Module Based
- Port Based

Step 3 Select **Device Based** and click **Go**.

The Devices and Tasks dialog box appears, with these panes:

Pane	Description
Device Selector	Select devices on which the NetConfig job has to run. You can select multiple device categories. For cable devices, you should select only one device for which you are creating the job.
Task Selector	Select the System-defined tasks or User-defined tasks that you want to run on the selected devices. All System-defined and User-defined tasks are categorized into various task groups. To select the tasks, expand the corresponding Task Group node. You can also search for a task or a group of tasks in the Task Selector by entering the Search expressions in the Search field. You can use the wildcard character "*" along with the Search expression. When you click the Search icon, the results are displayed in the Search Results tab. For descriptions of System-defined tasks and the device categories they support, see Using System-defined Tasks. For creating and using User-defined tasks, see Creating and Editing User-defined Tasks.

Step 4 Select the devices from the Device Selector pane. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 5 Select the tasks from the the Task Selector.

You can select one or more tasks at a time. Your selection will appear in the Selection pane.

Step 6 Click **Next.**

The Add Tasks dialog box appears with these panes:

Pane	Description
Applicable Tasks	Allows you to add a task. The tasks that you had selected using the Task Selector appear here. **Note** Of the tasks selected, only tasks that apply to the devices selected appear here. Select a task and click **Add** to create an instance for the task (see Step 7).
Added Instances	Allows you to edit the task instance you have added, view its CLI, or delete it. Select the instance of the task and click the required button (see Table 4-2).

The buttons available in this page are:

Table 4-2 Tasks Performed by Buttons in the Added Instances Pane

Buttons	Description
Edit	Task pop-up opens with previously assigned values. You can modify these values and click **Save**.

Table 4-2 Tasks Performed by Buttons in the Added Instances Pane (continued)

Buttons	Description
View CLI	Opens the Device Commands pop-up with the list of applicable devices and the corresponding CLI commands. Devices in your selection for which the commands are not applicable, are also displayed as Non-Applicable Devices. You can modify an instance of a configuration task (and its configuration commands) any time before the job is run.
Delete	Deletes the selected task instance.

Step 7 Select an applicable task and click **Add**.

The pop-up for the selected task appears.

Step 8 Set the parameters in the task dialog box and click **Save**.

(To reset the values that you have selected click **Reset**. Click **Cancel** to return to the previous dialog box, without saving your changes.)

You will see the instance of the task in the Added Tasks pane. The instance appears in the format:

Taskname_n, where *Taskname* is the name of the task you have added, and *n* is the number of the instance. For example, the first instance of a Banner task is `Banner_1`.

You can add as many instances as required, for a task.

Step 9 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 10 Set the schedule for the job, in the Scheduling pane:

Field	Description
Scheduling	
Run Type	Select the run type or frequency of the job—Immediate, Once, Daily, Weekly, Monthly, or Last Day of Month. If Job Approval is enabled, the Immediate option is not available.
Date	Select the start date for the job.
At	Select the start time for the job from the hour and minute drop-down lists.

Field	Description
Job Info	
Job Description	Enter the Job Description. This is mandatory. Make each description unique so you can easily identify jobs.
E-mail	Enter the e-mail addresses to which the status notices of the job will be sent. Separate multiple addresses with commas or semicolons. You must configure the SMTP server to send e-mails (**Admin > System > System Preferences**). Notification e-mails include a URL that displays the job details (see Viewing Job Details for more information on the details displayed). You need to be logged in to view the job details.
Comments	Enter your comments for the job. Comments appear in the job work order and are stored in the configuration archive.
Approver Comments	Enter comments for the job approver. This field is displayed only if you have enabled job approval for NetConfig. See *Administration of Cisco Prime LAN Management Solution 4.1* for more information.
Maker E-mail	Enter the E-mail ID of the job creator. This field is displayed only if you have enabled job approval for NetConfig. This is a mandatory field. See *Administration of Cisco Prime LAN Management Solution 4.1* for more information.

Step 11 Set the job options, in the Job Options pane.

Field	Description
Fail on Mismatch of Config Versions	Select to consider the job to be a failure when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job.
Sync Archive before Job Execution	Directs LMS archive running configuration before applying configuration changes.
Copy Running Config to Startup	Directs LMS to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Enable Job Password	
Login Username	Enter the Login Username. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.
Login Password	Enter the job password. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.

Field	Description
Enable Password	Enter the Enable password. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.
Failure Policy	Select one of these options to specify what the job should do if it fails to run on a device. • Stop on failure—If the job fails to execute on a device, the job is stopped. The database is updated only for the devices on which the job was executed successfully. • Ignore failure and continue—If the job fails on a device, the job skips the device and continues with the remaining devices. The database is updated only for the devices on which the job was executed successfully. • Rollback device and stop—Rolls back the changes on the failed device and stops the job. • Rollback device and continue—Rolls back the changes on the failed device and continues the job. • Rollback job on failure—Rolls back the changes on all devices and stops the job. See Configuring a Job to Roll Back on Failure.
Execution	Specify the order in which the job should run on the devices. • Parallel—Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time. • Sequential—Allows the job to run on only one device at a time. If you select sequential execution, you can click **Set Device Order** to set the order of the devices. In the Device Ordering dialog box: a. Select a device name b. Click **Move Up** or **Move Down** to change its place in the order. c. Click **OK** to save the current order and close the dialog box or Click **Cancel** to close the dialog box without making any changes.

Step 12 Click **Device Order** to view the device order.

The Set Device Order pop-up appears. You can reset the order in which the job should be executed on the devices using the Up and Down arrows.

When you are done, click **Done**. The pop-up closes.

Step 13 Click **Next**.

The Job Work Order dialog box appears with the general information about the job, the job policies, the job approval details (if you have enabled job approval), the device details, the task, and the CLI commands that will be executed on the selected devices as part of this job.

Step 14 Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A notification message appears along with the Job ID. The newly created job appears in the NetConfig Job Browser.

Create a NetConfig Job based on Module or Port

You can create a NetConfig job for ports or modules by selecting a port or module group from the Group Selector page in the NetConfig job flow.

You can create a NetConfig job for all devices in the port or module group, which is the default, or for a few devices in the port or module group. If devices are not available in the port or module groups, then Netconfig job will not be created and displays the following message `No devices in selected group`

To run the job for a few select devices, you need to select the devices from the Devices and Groups page and the port or module from the Group Selector page. The job will run for the selected devices provided the devices are available in the port or module selected. If there are no devices in Devices and Groups page, then the Netconfig job will be created only for the devices that are part of port or module groups.

To start a new NetConfig job based on Modules or Ports:

Step 1 Select either:

- **Configuration > Tools > NetConfig > Deploy**

Or

- **Configuration > Job Browsers > NetConfig**

The NetConfig Job Browser appears.

Step 2 Click **Create**.

The Netconfig Job Type page appears, displaying the following job flows:

- Device Based
- Module Based
- Port Based

Step 3 Either select:

- **Module Based**—To create a NetConfig job based on modules.

Or

- **Port Based**—To create a Netconfig job based on ports.

Step 4 Click **Go**.

The Device and Group Selector dialog box appears, with these options:

Options	Description
Device Selector	Allows you to select the devices on which the NetConfig job has to run. You can select multiple devices.
Group Selector	Allows you to select the device groups on which the NetConfig job has to run. You can select multiple device groups.

Step 5 Either:

- Select the devices using the Device Selector option.

Or

- Select the device groups using the Group Selector option.

You can also skip this page by clicking **Next** and directly go to Group Selector page.

Step 6 Click **Next**.

The Group Selector page appears displaying the Port or Module Groups dialog box with these options:

Options	Field/Button	Descriptions
Select Custom Group	Select the group on which the NetConfig job has to run. You can select multiple groups. • Module groups are displayed for a Module based NetConfig job. • Port groups are displayed for a Port based NetConfig job.	
Define an Adhoc Rule	Allows you to define Adhoc rules for a specific NetConfig job.	
	Object Type	Select the Object Type to form a group. • Module—This Object Type is listed only if you are creating a NetConfig job for modules. • Port—This Object Type is listed only if you are creating a NetConfig job for ports.
	Variable	Object type attributes, based on which you can define the group.
	Operator	Operator to be used in the rule. The list of possible operators changes based on the Variable selected. When using the *equals* operator the rule is case-sensitive.
	Value	Value of the rule expression. The possible values depend upon the variable and operator that you have selected. The value may be free-form text or a list of values. Wildcard characters are not supported.
	Add Rule Expression (Button)	Used to add the rule expression to the group rules.
	Rule Text	Displays the rule.
	Check Syntax (Button)	Verifies that the rule syntax is correct.
	Include (Button)	Lists all the modules or ports from the selected devices that are not matching the rule. You can later choose to include the modules or ports for group creation. Click **Include** to launch the Include List window.
	Exclude (Button)	Lists all the modules or ports from the selected devices that are matching the rule. You can later choose to exclude those modules or ports for group creation. Click **Exclude** to launch the Exclude List window.

Step 7 Click **Next**.

The Port or Module Tasks page appears.

Step 8 Select the following task using the Task Selector:

Port/Module Tasks	Description
GOLD Health Monitoring Test Task	Configure GOLD Health Monitoring tests on modules.
Adhoc Task	Configures user-defined commands on selected interfaces within a port group.
Manage Auto Smartports	Enables or disables Auto Smartports macros at port level.
Smartports	Applies Smartports macros at port level.
Catalyst Integrated Security Features	Configures port security features.
PoE Task	Configures power policies in ports.
EnergyWise Parameters Task	Configures EnergyWise in ports.
EnergyWise Events Task	Configures EnergyWise events in ports.
SRE Operation Task	Configures the following operations on Services Ready Engine (SRE) supported devices at port level: • Install—Install application in service modules. • Uninstall—Uninstall application from service modules. • Status—Displays the following: – Status of the service module – The applicable running on the module – Status of the installation and uninstallation being performed in the service module • Abort—Stop installation on a set of service modules in a SRE device. • Shutdown—Shutdown the set of service modules in a SRE device • Reset—Reset service modules in a SRE device.

Your selection appears in the Selection pane.

Step 9 Click **Next.**

The Add Tasks dialog box appears with these panes:

Pane	Description
Applicable Tasks	Allows you to add a task. The task that you selected using the Task Selector, appears here. From your selection, only the tasks that are applicable to at least one device that you have selected, appear here. Select a task and click **Add Instance** to create an instance for the task (see Step 10).
Added Instances	Allows you to edit the task instance you have added, view its CLI, or delete it. Select the instance of the task, and click the required button (see Table 4-3).

The buttons available in this page are:

Table 4-3 Tasks Performed by Buttons in the Added Instances Pane

Buttons	Description
Edit	Task pop-up opens with previously assigned values. You can modify the values.
View CLI	Device Commands pop-up opens with the list of applicable devices and their corresponding CLI commands. Devices in your selection for which the commands are not applicable, are also displayed as Non-Applicable Devices.

View Ports	Port Details pop-up opens showing the list of devices, their corresponding ports and the port group rule.
	For example,
	`Port Group: 100 Mbps Ethernet Ports`
	
	`Port Group Rule: Port.Speed = "100000000" AND  Port.Type = "6" IN Port.GROUP_ID = "/RME@rme-ch-dev-sf4/All Devices"`
	
	`Ports matching the port group rule:`
	`4/1`
	`4/2`
	`4/3`
	`4/4`
	`4/5`
	`4/6`
	`4/7`

Delete	Deletes the selected task instance.

Step 10 Select the applicable task and click **Add**.

The pop-up for the selected task appears.

Step 11 Set the parameters in the Task dialog box and click **Save**.

You will see the instance of the task in the Added Tasks pane of the Add Tasks dialog box. The instance appears in the format:

Taskname_n, where *Taskname* is the name of the task you have added, and *n* is the number of the instance. For example, the first instance of a Banner task is `Banner_1`.

You can add as many instances as required, for a task.

Step 12 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 13 Set the schedule for the job, in the Scheduling pane:

Field	Description
Scheduling	
Run Type	Select the run type or frequency for the job—Immediate, Once, Daily, Weekly, Monthly, or Last Day of Month.
Date	Select the start date for the job.
at	Select the start time for the job from the hour and minute drop-down lists.
Job Info	
Job Description	Enter the Job Description. Make each description unique so you can easily identify jobs. This is mandatory.
E-mail	Enter e-mail addresses to which the job will send status notices. Separate multiple addresses with commas or semicolons. You must configure the SMTP server to send e-mails (**Admin > System > System Preferences**). Notification e-mails include a URL that displays the job details. See Viewing Job Details. If you are not logged in, you must log in using the provided login panel to view the job details.
Comments	Enter your comments for the job. Comments appear in job work order and are stored in configuration archive.
Approver Comments	Enter comments for the job approver. This field is displayed only if you have enabled job approval for NetConfig. See *Administration of Cisco Prime LAN Management Solution 4.1* for more information.
Maker E-mail	Enter the e-mail-ID of the job creator. This field is displayed only if you have enabled job approval for NetConfig. This is a mandatory field. See *Administration of Cisco Prime LAN Management Solution 4.1* for more information.

Step 14 Set the job options, in the Job Options pane.

Field	Description
Fail on Mismatch of Config Versions	Select to cause job to be considered a failure when the most recent configuration version in the archive is not identical to the most recent configuration version that was in the archive when you created the job.
Sync Archive before Job Execution	Select to cause job to archive running configuration before making configuration changes.
Copy Running Config to Startup	Select to cause job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Enable Job Password	
Login Username	Enter the Login Username. This option is available if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of LMS.

Field	Description
Login Password	Enter the job password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you entered at the time of adding the device in the Device and Credentials Administration module of LMS.
Enable Password	Enter the Enable password. This option is available if you have set the appropriate job password policy in the Configuration Management module. This option overrides the credentials that you entered at the time of adding the device in the Device and Credentials Administration module of LMS.
Failure Policy	Select one of these options to specify what the job should do if it fails to run on a device. • Stop on failure—If the job fails to execute on a device, the job is stopped. The database is updated only for the devices on which the job was executed successfully. • Ignore failure and continue—If the job fails on a device, the job skips the device and continues with the remaining devices. The database is updated only for the devices on which the job was executed successfully. • Rollback device and stop—Rolls back the changes on the failed device and stops the job. • Rollback device and continue—Rolls back the changes on the failed device and continues the job. • Rollback job on failure—Rolls back the changes on all devices and stops the job. See Configuring a Job to Roll Back on Failure
Execution	Specify the order in which the job should run on the devices. • Parallel—Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time. • Sequential—Allows the job to run on only one device at a time. If you select sequential execution, you can click **Set Device Order** to set the order of the devices. In the Device Ordering dialog box: a. Select a device name b. Click **Move Up** or **Move Down** to change its place in the order. c. Click **OK** to save the current order and close the dialog box or Click **Cancel** to close the dialog box without making any changes.

Step 15 Click **Device Order** to view the device order. The Set Device Order pop-up appears.

You can reset the order in which the job should be executed on the devices using the up and down arrows.

Step 16 Click **Next**.

The Job Work Order dialog box appears with:

- General information about the job
- Job policies
- Job approval details (if you have enabled job approval)
- Device details

- Task
- CLI commands that will be executed on the selected devices as part of this job
- Rule Expression (applicable for Adhoc groups).

Step 17 Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A notification message appears along with the Job ID. The newly created job appears in the NetConfig Job Browser.

Browsing and Editing Jobs Using the NetConfig Job Browser

You can browse the NetConfig jobs that are registered on the system. Using the NetConfig Job Browser, you can also manage NetConfig jobs (create, edit, copy, retry, stop, or delete).

To create and start a new NetConfig job, see Starting a New NetConfig Job.

Note View Permission Report (**Reports > System > Users > Permission**) to check whether you have the required privileges to perform this task.

To invoke the NetConfig Job browser that lists all the scheduled report jobs, select either:

- **Configuration > Tools > NetConfig > Deploy**

Or

- **Configuration > Job Browsers > NetConfig**

.The columns in the NetConfig job browser displays the following information:

Column	Description
Job ID	Unique number assigned to a job when it is created. For periodic jobs such as Daily, Weekly, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001. Click on the hyperlink to view the Job details. See Viewing Job Details.
Status	Status of the job: • Successful—When the job is successful. • Failed—When the job has failed. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed amounts to 5. • Cancelled—When the job has been stopped. • Running—When the job is in progress. • Waiting—When the job is waiting for approval (if job approval has been enabled). • Rejected—When the job has been rejected (if job approval has been enabled).

Column	Description
Description	Description of the job, entered at the time of job creation.
Owner	Username of the job creator.
Scheduled at	Date and time at which the job was scheduled.
Completed at	Date and time at which the job was completed.
Flow Type	Type of the job flow—Port, Module, Device.
Schedule Type	Type of job schedule—Immediate, Once, Daily, Weekly, Monthly, Last day of the month. You can specify when you want to run the NetConfig job. To do this, select one of these options from the drop-down menu: • Immediate—Runs the report immediately. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. • Last Day of the Month—Runs the job on the last day of the month, beginning with the month that you specify. For periodic jobs, the subsequent instances will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.

You can filter the jobs using the Filter by field in the NetConfig Job Browser using any of the following criteria:

Filter Criteria	Description
All	Select All to display all jobs in the job browser
Job ID	Select Job ID and enter the Job ID that you want to display. For non-periodic jobs, the specified Job ID appears in the browser. For periodic jobs, all the instances of the selected Job ID will also be displayed in the browser.
Status	Select Status and then select any one of these: • Successful • Failed • Cancelled • Running • Scheduled • Approved • Waiting • Rejected

Filter Criteria	Description
Description	Select Description and enter the first few letters or the complete description.
Owner	Select Owner and enter the user ID or the beginning of the user ID.
Schedule Type	Select the schedule type and select any one of these: • Immediate • Once • Daily • Weekly • Monthly • Last day of the month
Flow Type	Select Flow Type and then select any one of these: • Device • Port • Module
Refresh (Icon)	Click this icon to refresh the NetConfig job browser.

You can schedule a default purge job to purge the records of NetConfig jobs.

You can perform the following operations using the NetConfig job browser. (See Table 4-4):

Table 4-4 Operations Using the NetConfig Job Browser

Button	Description	Usage Notes
Edit	Edits the selected pending job. • For Device based jobs, the Job definition opens at the Devices and Tasks dialog box, with current information about the job. • For Module based jobs, the Job definition opens at the Devices and Groups dialog box, with current information about the job. • For Port based jobs, the Job definition opens at the Devices and Groups dialog box, with current information about the job. You can edit a job the same way you define and schedule a new job. See Starting a New NetConfig Job. The Job ID of an edited job remains unchanged.	Unless you own a job, your login ID determines whether you can use this option. If the job start time occurs during editing, it runs without edits. You can complete the edits and schedule the job to run again, but you cannot re-edit the job. To prevent the job from running without edits, either: • Complete your edits before the job start time. Or • Cancel the job and create a new one.

Table 4-4 Operations Using the NetConfig Job Browser (continued)

Button	Description	Usage Notes
Copy	Copies selected job. You can copy a job and give it a new schedule. • For Device based jobs, the Job definition opens at the Devices and Tasks dialog box, with all the selections for the job that you are copying. • For Module based jobs, the Job definition opens at the Devices and Groups dialog box, with all the selections for the job that you are copying. • For Port based jobs, the Job definition opens at the Devices and Groups dialog box, with all the selections for the job that you are copying. You can copy a job in the same way you define and schedule a new job. See Starting a New NetConfig Job. A new Job ID with the copied job details is created.	-
Retry	Retry a failed job. • For Device based jobs, the Job definition opens at the Devices and Tasks dialog box. You can edit the job the same way as you would define and schedule a new job. However, you cannot add new devices or change the tasks for the job that you are retrying. You can select a few of the failed devices to retry the job. • For Module based jobs, the Job definition opens at the Devices and Groups dialog box. You can edit the job the same way as you would define and schedule a new job. However, you cannot add new devices, modules or change the tasks for the job that you are retrying. You can select a few of the failed devices to retry the job. • For Device based jobs, the Job definition opens at the Devices and Groups dialog box. You can edit the job the same way as you would define and schedule a new job. However, you cannot add new devices, ports or change the tasks for the job that you are retrying. You can select a few of the failed devices to retry the job.	Unless you own the job, your login determines whether you can use this option. There may be some devices whose configuration has been downloaded. However, their running configuration has not been written to the Startup configuration. You can perform Retry Job on these devices just as you can on a failed job.

Table 4-4 Operations Using the NetConfig Job Browser (continued)

Button	Description	Usage Notes
Stop	Stops or cancels a running job. You will be asked to confirm the cancellation of the job. However, the job will be stopped only after the devices currently being processed are successfully completed. This is to ensure that no device is left in an inconsistent state. If the job that you want to stop is a periodic job, you will also be asked whether you want to cancel all the instances of the job. Click **OK** to cancel all instances. If you click **Cancel**, only the selected instance of the job is cancelled. The next instance of the job will appear in the Job browser with the status `Scheduled`.	Unless you own the job, your login determines whether you can use this option. You cannot restart the stopped job. You can however copy the stopped job and Job ID.
Delete	Deletes the selected job from the job browser. You can select more than one job to delete. You will be asked to confirm the deletion. If the job that you have selected for deletion is a periodic job, this message appears: `If you delete periodic jobs, or instances of a periodic job, that are yet to be run, the jobs will no longer run, nor will they be scheduled to be run again. You must then recreate the deleted jobs. Do you want to continue?` Click **OK** to confirm the deletion. The selected job will be deleted. You can delete a job that has been successful, failed, or stopped, but you cannot delete a running job.	Unless you own the job, your login determines whether you can use this option. You must stop a running job before you can delete it.

Viewing Job Details

You can learn more about any job by viewing its details.

Step 1 Go to the NetConfig Job Browser and click the Job ID hyperlink. See Starting a New NetConfig Job to invoke the NetConfig Job Browser.

The Job Details pop-up appears, displaying the day, date and time details in the header at the top of the report. The Job ID and the Status appear in the header of the report.

The Job Details dialog box has two panes. The left pane contains a table of contents for the job results. The results appear in the right pane.

Step 2 Click a content in the left pane to view its corresponding report in the right pane.

Step 3 Click expand and collapse icons to open and close the folder tree in the left pane.

If a folder has subfolders, the next level of subfolders appears under it. Otherwise, its corresponding report appears in the right pane.

The contents of the left pane depends on the state of the job. The left pane can contain:

- Job Summary (in the Job Details folder).
- Downloaded Devices (in the Device Details folder).
- Work Order

Page/Folder	Description	
Job Details	Job Summary	Click to display summary of completed job: • Job Summary: – Status – Start Time – End Time • Job Messages: – Pre-job Execution – Post-job Execution • Device Update: – Successful – Failed – Not attempted – Pending – Devices Pending Registration for Smart Call Home (SCH) The URL https://tools.cisco.com/sch/pendingDevices.do is displayed only for SCH NetConfig jobs. Click the URL to register the devices that are pending to process SCH messages at Cisco.com. For more information on Devices Pending Registration for SCH, see the Smart Call Home User Guide at: http://www.cisco.com/en/US/services/ps2827/ps2978/ps7334/networking_solutions_products_genericcontent0900aecd806f52c2.pdf
Device Details	Downloaded Devices	Contains detailed job results for each device in a table: • Device—List of devices on which the job ran. • Status—Status of job (success, failure, etc.) • Message—A message about the status of a job. – If the job failed on the device, the reason for failure is displayed. – If the job was successful on the device, the message `Deploy Successful` is displayed. You can filter the devices by selecting a status and clicking **Filter**. This page displays the number of rows you have set for display in the Rows per Page field. You can increase the rows up to 500 in each page. You can navigate among the pages of the report using the navigation icons at the right bottom of this table. Click on a device to view the details such as protocol, status and reason when applicable, task used and the CLI output for that device. These details appear in a pop-up window. Double-click to display status folders that correspond to possible device status.

Page/Folder	Description
StatusFolder	
Update Successful	Devices that were successfully updated.
Update Failed	Devices that were not updated. Includes devices on which rollback was attempted, regardless of whether the rollback was successful.
Not Attempted	Job did not try to update devices, even though they were selected. Usually occurs when a previous device failed and failure property was set to Stop on Failure.
Work Order	Click to display Job Work Order, which contains the same information as the workorder that was displayed when the job was created. (For the workorder details, see Step 16 in Starting a New NetConfig Job). For retried jobs, the job definitions are not updated. For such jobs, the original job definitions are retained.
ViewPorts (button)	Port Details pop-up opens showing the list of devices, their corresponding ports and the group rule. The View Ports button is available only for jobs that are either in Scheduled, Waiting for Approval, or in Rejected states.

To perform actions, click one of the following (For detailed descriptions of these operations see Operations Using the NetConfig Job Browser in Table 4-4):

- Edit
- Copy
- Retry
- Stop
- Delete

Creating and Editing User-defined Tasks

You can create User-defined Tasks and add one or more templates to each task.

The template, in turn, is associated with the Meta-Data Framework (MDF) categories of devices, for which these templates will be applicable.

The templates contain configuration commands and rollback commands (see Creating Rollback Commands). You can enter the configuration commands either by typing them or by importing them from a file.

You can create a new task and add one or more templates to it. You can also add templates to an existing task. Name a task when you create it and as it is saved for future use. You can copy, edit, and reuse your tasks. You can assign access privileges to tasks while or after you create them (see Assigning Tasks to Users).

You cannot add User Defined Templates to System Defined Tasks.

After you have successfully created a User-defined Task, this task will appear under the User-defined Tasks group in the Task Selector of the NetConfig Job creation wizard. You can create a NetConfig job using the User-defined task. For details on the Task Selector and job creation, see Step 2 in Starting a New NetConfig Job.

For each template, you should specify all the information including the configuration commands, rollback commands (see Rolling Back Configuration Changes), mode (Config or Enable), and the device category for which these commands will be applicable.

At the time of job creation, you should ensure that the User-defined task that you have selected is applicable to the MDF categories of the devices that you have selected.

If the task that you have selected does not apply to the categories of any of the devices that you have selected, it will not be displayed in the Applicable Tasks pane of the NetConfig job wizard, during job creation.

For example, if you have selected an CatalystOS category of device, but selected a user-defined task that is applicable to a Cable device, then the task will not appear in the Applicable Tasks pane of the job wizard and you will not be able to proceed further with the job creation. For details on the Applicable Tasks pane and job creation, see Step 6 in Starting a New NetConfig Job

Caution NetConfig does not validate the commands you enter in a user-defined template within a task. If you enter incorrect commands you might misconfigure or disable the devices on which the job using the template runs.

View the Permission Report (**Reports > System > Users > Permission**) to check whether you have the required privileges to perform this task.

Step 1 Select **Configuration > Tools > NetConfig > User Defined Tasks**.

The User-defined Tasks dialog box appears. If you are creating a task for the first time, the system displays a message that there are no user-defined tasks.

The User-defined Tasks dialog box has a Tasks browser in its left pane. After you create a task, the task is displayed in the Tasks browser along with its templates.

Step 2 Define or edit a User-defined task by entering the following information in the dialog box.

Area/Field/Button	Description	Usage Notes
Name	Enter name for the new task. This is a mandatory field.	To create new task from a copy of an existing task: 1. Select the name from Templates list, 2. Enter the new name. 3. Save the task. To modify a task, select it from the tasks list but do not modify its name. You can modify a task by adding or deleting templates, modifying existing templates and changing other details.
Template Name	Enter the template name. This is a mandatory field.	Template Name is provided for User Defined Tasks when you create a template for more than one device category which has different commands to execute.

Area/Field/Button	Description	Usage Notes
Command Mode	Select mode (config or enable) in which commands will run.	Each user-defined template can run commands in one mode only. If you select **Enable**, enter Rollback Commands area is disabled because only config commands can be rolled back.
Parameterized	Select Parameterized if you want to create a parameterized template.	The template parameters will be picked up from a file that you specify, at the time of scheduling a job using this task. See "Parameterized Templates".
Device Type	Select device category template will configure.	You can associate any number of MDF categories with a template, if the command is applicable to them.
CLI Commands	Enter configuration commands or select the configuration commands file. The configuration commands file should reside in the default location: On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/netconfig/cmdFiles/ On Windows: *NMSROOT*\files\rme\netconfig\cmdFiles Where, *NMSROOT* is the LMS install directory. If you want to import the configuration commands from an existing file, enter the default file location in the Import from File field. Alternatively, when you click on the Browse button, a file browser opens with the default location of the configuration commands file. You cannot change this default import directory.	To enter configuration commands, do any of the following: • Type in larger text box, one command in each line. Or • Enter enter the default file location of the configuration command files in the Import from File field. • Click **Browse.** A file browser opens with the default location of the configuration commands file. You cannot change this default import directory. You can also enter interactive commands and multi-line commands. See Handling Interactive Commands.

Area/Field/Button	Description	Usage Notes
Rollback Commands	Enter configuration commands for the template to run when the job fails and the failure policy is set to the rollback option. If you want to import the rollback commands from an existing file, enter the file location in the Import from File field. The rollback commands file should reside in the default location: On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/netconfig/cmdFiles/ On Windows: *NMSROOT*\files\rme\netconfig\cmdFiles Where, *NMSROOT* is the LMS install directory. Alternatively, when you click on the Browse button, a file browser opens with the default location of the rollback commands file. You cannot change this default import directory.	To enter rollback commands, do any of the following: • Type in larger text box, one command in each line. • Enter the default file location of the rollback command files in the Import from File field. • Click **Browse.** A file browser opens with the default location of the configuration commands file. You cannot change this default import directory.

- Click **Save** to save the task with the current information.

  Or

- Click **Delete** to delete the current task from the system.

To cancel the user-defined task you are creating, select a command from the Jobs or Admin menu (or a corresponding button) and click **Yes** in the resulting dialog box.

To add a user-defined task, select Select **Configuration > Tools > NetConfig > User Defined Tasks**. The User-defined Tasks dialog box appears with no values.

To copy a user-defined task:

Step 1 Select the task from the Tasks browser.

The details appear in the right pane of the User-defined Tasks dialog box.

Step 2 Change the name of the Task and click **Save**.

To modify a user-defined task:

Step 1 Select the task from the Tasks browser.

The details appear in the right pane of the User-defined Tasks dialog box.

Step 2 Select templates associated with the task from the Task browser, and modify them

You can change details such as the command mode, parameterization option, the device type, the CLI commands or the rollback commands.

You can add a template or delete an existing one. When you click Save, a message appears that the task is modified.

This section contains:

- Parameterized Templates
- Creating a Parameters File (XML file)
- Parameters File: More Examples

Parameterized Templates

You can include parameterized templates within User-defined tasks. A parameterized template allows the configuration commands in the templates to contain user-defined variables.

Multiline feature of parameterized templates is not supported. However, interactive command deploy is supported.

You can select the Parameterized option when you create a User-defined task (see Creating and Editing User-defined Tasks).

If you select the Parameterized option, you should enter the actual values for the parameters in the template in a separate Parameters file (see Creating a Parameters File (XML file)) when you create a NetConfig job (see Creating and Editing User-defined Tasks). The Parameters file is the XML file that contains the parameter values.

The Parameters file should reside on the server at this location:

- *NMSROOT*\files\rme\netconfig\cmdFiles (On Windows)
- /var/adm/CSCOpx/files/rme/netconfig/cmdFiles/ (On Solaris and Soft Appliance)

where *NMSROOT* is the LMS install directory.

To create a Parameterized User-defined task and apply this in a NetConfig job:

Step 1 Create a User defined Task with variables embedded in the command body. For details see Creating and Editing User-defined Tasks.

For example:

You can enter the command **`ntp server`** *`$ntpServer`* in the CLI Commands text box in the User-defined Tasks dialog box.

Step 2 Select the Parameterized check box in the User-defined Tasks dialog box.

Step 3 Click **Save** to save your User-defined Parameterized task.

Step 4 Create the Parameters file (XML file) containing the values for *$ntpServer* task. For details, see Creating a Parameters File (XML file).

For example:

```
<DEVICE NAME = 10.76.38.54>
<CMDPARAM NAME = ntpServer>
<value>mytimeserver</value>
</CMDPARAM>
</DEVICE>
```

Step 5 Repeat the above step in the Parameters file, for all the devices that you plan to include in the job, if each device refers to a different *ntpServer*.

Alternatively, you can have a global section if that variable does not change for each device. For details, see Creating a Parameters File (XML file).

Step 6 Store the Parameters file in:

- *NMSROOT*\files\rme\netconfig\cmdFiles directory (On Windows)
- /var/adm/CSCOpx/files/rme/netconfig/cmdFiles/ (On Solaris and Soft Appliance)

  where *NMSROOT* is the LMS install directory.

Step 7 Create a NetConfig job and select your User-defined Parameterized task. For details see Starting a New NetConfig Job.

You are prompted to enter the filename while adding the task to the NetConfig job.

You can check the syntax of the text file that contains the parameters. To do this, select **Check Syntax**.

Step 8 Complete the job creation. For details, see Creating and Editing User-defined Tasks.

Creating a Parameters File (XML file)

A specific format is defined for embedding variables in User-defined tasks and the corresponding Parameters file that contains the values for the parameters.

The variables in the User-defined tasks, which you enter in the CLI Commands text area of the User-defined Tasks dialog box (see Creating and Editing User-defined Tasks), should be preceded by `$`.

For example, for an NTP server parameter, it should be: `$ntpServer`

Similarly, the Parameters file also follows a specified format.

Here is the sample format and example of the Parameters file (the XML command file that contains the values for the parameters) for a parameterized template:

```
<GLOBAL>
<CMDPARAM NAME = password>
<value>abc</value>
</CMDPARAM>
<CMDPARAM NAME = message>
<value>test all</value>
</CMDPARAM>
</GLOBAL>

<DEVICE NAME = 10.76.38.54>
<CMDPARAM NAME =  ntpServer>
<value>ServerName</value>
</CMDPARAM>
</DEVICE>
```

You can assign the device-specific values to variables in the <DEVICE> area. If there are no device-specific values, the default values in the <GLOBAL> area are considered as actual values for these variables. You do not need to add a <GLOBAL> area in the Parameters file if you are referencing each device explicitly (using the <DEVICE> area for each device).

Parameters File: More Examples

This section gives more examples of the format of the text to be entered in the CLI Commands body at the time of creating a User-defined Task, and the commands to be entered in the corresponding Parameters file.

For example, you can enter these parameters while creating a User-defined task, in the CLI Commands text box:

`ntp server` *ntpServer*

`ip http port` *portValue*

`ip address` *ipAddress*

In the corresponding Parameters file, which is stored under:

- *NMSROOT*\files\rme\netconfig\cmdFiles directory (On Windows)
- /var/adm/CSCOpx/files/rme/netconfig/cmdFiles/ (On Solaris and Soft Appliance)

where *NMSROOT* is the LMS install directory, enter:

```
<GLOBAL>
<CMDPARAM NAME = ntpServer>
<value>10.10.10.10</value>
</CMDPARAM>
<CMDPARAM NAME = portValue>
<value>90</value>
</CMDPARAM>
<CMDPARAM NAME = ipAddress>
```

```
<value>1.1.1.1</value>
</CMDPARAM>
</GLOBAL>

<DEVICE NAME = 10.76.38.54>
<CMDPARAM NAME = ntpServer>
<value>20.20.20.20</value>
</CMDPARAM>
<CMDPARAM NAME =  portValue>
<value>55</value>
</CMDPARAM>
</DEVICE>

<DEVICE NAME = 10.77.202.229>
<CMDPARAM NAME = ntpServer>
<value>30.30.30.30</value>
</CMDPARAM>
</DEVICE>
```

In such a case, when the NetConfig job contains the device 10.76.38.54, the following commands are generated:

`ntp server 20.20.20.20` (taken from the device-specific section of the Parameters file)

`ip http port 55` (taken from the device-specific section of the Parameters file)

`ip address 1.1.1.1` (taken from the global section of the Parameters file)

When the job contains the device 10.77.202.229, the following commands are generated:

`ntp server 30.30.30.30` (taken from the device-specific section of the Parameters file)

`ip http port 90` (taken from the global section of the Parameters file)

`ip address 1.1.1.1` (taken from the global section of the Parameters file)

When the job contains other devices, all the values are taken from the global section of the XML file, and the following commands are generated:

```
ntp server 10.10.10.10
ip http port 90
ip address 1.1.1.1
```

If the value for a parameter is not found in the command file, the syntax check (in the job creation flow) displays an error.

You can enter any special character, except <, >, and $, that is accepted by the device as the value for a parameter in the command file. This is because NetConfig does not process the parameter values. NetConfig only reads the value given between `<value>` and `</value>` tags and generates the command.

Assigning Tasks to Users

You can assign access privileges to NetConfig tasks, to users with Network Operator privileges or lesser. All other users with privileges higher than Network Operator are assigned all tasks by default.

A network administrator must assign task access privileges to other users. See Understanding NetConfig User Permissions section for details.

Note View the Permission Report (**Reports > System > Users > Permission**) to check whether you have the required privileges to perform this task.

To assign tasks to users:

Step 1 Select **Configuration > Tools > NetConfig > Assigning Tasks**.

The Assign Tasks dialog box appears.

Step 2 Enter the username of the user to whom you want to assign the tasks.

This should be a valid LMS user.

Step 3 Select the task that you want to allocate to the user from the Available tasks list box and click **Add**.

You can select more than one task, by holding down the Shift key while selecting the task.

The selected tasks appear in the Selected Tasks list box.

To remove assigned tasks, select the tasks from the Selected Tasks list box and click **Remove**.

Step 4 Add all the required tasks to the Selected Tasks list box.

Step 5 Click **Assign** to assign the task access privileges to the specified user.

For a specified user, to see the assigned tasks, enter the username in the Username field and click **Show Assigned**.

The tasks assigned to the user appear in the Selected Tasks list box.

Step 6 Click **Report** to generate the User Task Report.

The User Task Report shows the list of users and the tasks assigned for each user.

Note By default, all the tasks are assigned to admin users. Therefore, the User Task Report will not list the users with Admin privileges.

Handling Interactive Commands

An interactive command is the input you will have to enter, following the execution of a command.

For example, on a Catalyst device, a clear counters command on a Cat 5000 will give the following output:

```
c5000# (enable) clear counters. This command will reset all MAC and port counters reported
in CLI and SNMP. Do you want to continue (y/n) [n]?
```

In LMS, such commands can be included in config jobs executed via NetConfig or ConfigEditor. For more details also see Editing and Deploying Configurations Using Config Editor.

You can handle interactive commands using NetConfig user-defined templates, and by using Adhoc tasks. See Using NetConfig User-defined Templates and Adhoc Tasks.

You cannot run interactive commands through NetConfig CLI.

Using NetConfig User-defined Templates and Adhoc Tasks

You can enter an interactive command in the Enter CLI Commands area, using the following syntax:

CLI Command`<R>`*command response 1* `<R>`*command response 2*

`<R>` tag is case-sensitive and this must be entered in uppercase only.

Example

For a Catalyst device, a **`clear counters`** command will give the following output

```
c5000# (enable) clear counters This command will reset all MAC and port counters reported
in CLI and SNMP. Do you want to continue (y/n) [n]?
To clear the counter, the syntax is:
clear counters <R>y
To accept the default, the syntaxes are:
clear counters <R>n
or
clear counters <R>
```

To accept the default value, you do not need to enter any values after the tag `<R>`.

Handling Multi-line Commands

You can enter multi-line commands as a part of User-defined and Adhoc tasks. The multi-line commands must be within the tag <MLTCMD> and </MLTCMD>.

These tags are case-sensitive and you must enter them only in uppercase. You cannot start this tag with a space.

Example

```
<MLTCMD> banner login "Welcome to
Cisco Prime LMS
Essentials - you are using
Multi-line commands" </MLTCMD>
```

You can have a blank line within a multi-line command. The commands within the MLTCMD tags are considered as a single command and will be downloaded as a single command onto the device.

Using System-defined Tasks

NetConfig provides System-defined configuration tasks. You can create configuration commands by using these tasks (see Understanding the System-defined Task User Interface (Dialog Box)).

Each task supports one or more device categories (see Table 4-5). Table 4-5 displays a comprehensive list of all templates available and a brief description of each.

- For Device-based jobs, the System-defined tasks are available in the Devices and Tasks dialog box of the NetConfig job wizard.
- For Port-based jobs, the System-defined tasks are available in the Port Tasks page of the NetConfig job wizard.
- For Module-based jobs, the System-defined tasks are available in the Module Tasks page of the NetConfig job wizard.

All System-defined tasks are categorized into various task groups in the Tasks Selector. To select the tasks, you must expand the corresponding Task Group node.

After you select the devices and the tasks and click **Next** (see Starting a New NetConfig Job), the selected tasks appear in the Applicable Tasks pane of the Add Tasks dialog box (in the Job wizard).

When you select an applicable task and click **Add Instance**, a dialog box appears for the selected System-defined configuration task.

This is a dynamic user interface. The task dialog box displays parameters, based on the devices that you selected in Device Selector.

For example, if you have selected IOS devices, you can specify IOS parameters in this dialog box. If not, this section will not be available to you.

When you enter information in the fields of the task and click **Save**, the task appears as a numbered instance in the Added Instances pane of the Add Tasks dialog box.

For the detailed procedure and for information on how to edit the task instances, view CLI, or delete the instances, see Starting a New NetConfig Job.

You can add multiple instances of a configuration task to a job by selecting an applicable task, adding information, and saving this information. You need to do this whenever you add instances. However, you can include only one instance of a task in a job.

Each System-defined task also creates Rollback commands that you can use to roll back the changes to devices if the job fails.

- View the Permission Report (**Reports** > **System** > **Users** > **Permission**) to check whether you have the required privileges to perform this task.
- If you use TFTP protocol to deploy NetConfig templates to devices, the DCR does not reflect the updates.

Table 4-5 NetConfig System-Defined Tasks Supported by LMS Device Categories

Task Group	Task	Description	IOS	CatOS	CSS	CE	NAM	PIX	Cable
General	Adhoc Task	Enter any configuration commands as required.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Authentication Proxy Task	Configure Authentication Proxy.	Yes	-	-		-	-	Yes
	Banner Task	Add, remove, or edit banners.	Yes	Yes	-		-	-	Yes
	CDP Task	Configure Cisco Discovery Protocol (CDP).	Yes	Yes	-	Yes	-	-	Yes
	DNS Task	Configure DNS.	Yes	Yes	Yes	Yes	Yes	-	Yes
	HTTP Server Task	Configure HTTP access on VPN devices.	Yes	Yes	-	-	-		Yes
	IGMP Configuration Task[1]	Configure IGMP of selected cable interfaces.	-	-	-	-	-	-	Yes
	Internet Key Exchange (IKE) Configuration Task[2]	Configure IP security (IPSec).	Yes	-	-	-	-	Yes	Yes
	Interface IP Address Configuration Task	Configure IP interface address of selected interface.	-	-	-	-	-	-	Yes
	NTP Server Configuration Task	Configure Network Time Protocol (NTP).	Yes	Yes	Yes	Yes	-	-	Yes
	RCP Configuration Task	Configure rcp	Yes	-	-	-	-	-	Yes
	Reload Task	Reload devices	Yes	-	-	Yes	Yes	-	Yes
	Smart Call Home Task	Register devices with Cisco Smart Call Home	Yes	-	-	-	-	-	-
	Syslog Task	Configure Syslog message logging.	Yes	Yes	Yes	Yes	-	Yes	Yes
	Transform System-Defined Task	Configure IPSec.	Yes	-	-	-	-	Yes	Yes
	User-defined Protocol Task	Configure the User-defined protocol on NAM devices.	-	-	-	-	Yes	-	-
	Web User Task	Configure the web user for NAM devices	-	-	-	-	Yes	-	-

Table 4-5 NetConfig System-Defined Tasks Supported by LMS Device Categories

Task Group	Task	Description	IOS	CatOS	CSS	CE	NAM	PIX	Cable
Cable	Cable BPI/BPI+ Task	Assign self-signed certificate, configure cable interface, and set BPI/BPI+ options.	-	-	-	-	-	-	Yes
	Cable DHCP-GiAddr and Helper Task[1]	Configure DCHP-GiAddr and Helper Address of the selected cable interface.	-	-	-	-	-	-	Yes
	Cable Downstream Task[1]	Activate/Deactivate DS Ports, Interleave Depth, MPEG Framing Format, Modulations, Channel ID and Frequency of the selected cable interfaces.	-	-	-	-	-	-	Yes
	Cable Interface Bundling Task[1]	Configure Interface Bundling on selected cable interface.	-	-	-	-	-	-	Yes
	Cable Spectrum Management Task	Assign Spectrum Groups and Interfaces on a selected cable interface.	-	-	-	-	-	-	Yes
	Cable Trap Source Task	Configure SNMP Traps hosts, notification, message and notification of SNMP Traps on a cable interface.	-	-	-	-	-	-	Yes
	Cable Upstream Task[1]	Activate and configure upstream on selected cable interfaces.	-	-	-	-	-	-	Yes
Credential	Enable Password Task	Configure, or change enable or secret password to enter in enable mode on devices.	Yes	Yes	-	-	-	Yes	Yes
	Local Username Task	Configure local username and password authentication on devices.	Yes	-	Yes	-	-	-	Yes
	SSH Configuration Task	Configure SSH.	Yes	-	Yes	Yes	Yes		Yes
	Telnet Password Configuration Task	Add, remove, and edit Telnet passwords.	Yes	Yes	-	-	-	Yes	Yes
Encryption	Certification Authority Task[2]	Create, or modify Certification Authority. Provides manageability and scalability for IP security (IPSec) standards on VPN devices.	Yes	-	-		-	-	Yes
	Crypto Map Task[2]	Configure IPSec.	Yes	-	-	-	-	Yes	Yes
EEM	Embedded Event Manager Task	Configure EEM Scripts or Applets on the devices	Yes	-	-	-	-	-	-
	EEM Environmental Variables Task	Configure EEM Environmental Variables on the devices	Yes	-	-	-	-	-	-
EnergyWise	EnergyWise Configuration Task	Configure EnergyWise in Devices	Yes	-	-	-	-	-	-

Table 4-5 NetConfig System-Defined Tasks Supported by LMS Device Categories

Task Group	Task	Description	IOS	CatOS	CSS	CE	NAM	PIX	Cable
GOLD	GOLD Boot Level Task	Configure Boot Level Diagnositc tests on the devices	Yes	-	-	-	-	-	-
	GOLD Monitoring Test Task	Configure GOLD Monitoring tests on devices	Yes	-	-	-	-	-	-
SNMP	SNMP Community Configuration Task	Add, remove, and edit SNMP community strings	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	SNMP Security Configuration Task	Configure SNMP Security feature on devices.	Yes	-	-	Yes	-	-	Yes
	SNMP Traps Configuration Task	Configure SNMP traps.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Port Macros	Auto Smartports	Configure Auto Smartport macros on devices.	Yes	-	-	-	-	-	-
TACACS	TACACS Configuration Task	Configure TACACS authentication.	Yes	-	-		-	-	Yes
	TACACS+ Configuration Task	Configure TACACS+ authentication	Yes	Yes	-	Yes	Yes	-	Yes
	RADIUS Server Configuration Task	Configure RADIUS server and task.	Yes	-	Yes	Yes	-	-	Yes
User-defined Tasks		Lists all user-defined tasks							

1. You can apply this task only to a single device, at a time because cable templates configure interfaces on devices.
2. You must follow this sequence to complete the configuration of the IPSec on devices:

a. IKE configuration System-defined task.

b. Transform System-defined task.

c. Crypto Map System-defined task.

Understanding the System-defined Task User Interface (Dialog Box)

NetConfig tasks support devices in the following device categories:

- IOS
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS
- Cable

Each of the system-defined tasks have their own dynamic user interface, or dialog box, that displays fields for a specified category of devices only if you have selected that category of device.

The dialog boxes for system-defined tasks may have these groups, links, and buttons:

- Common Parameters—This group of fields appears at the top of the task dialog box. In the fields under this group, you can enter the parameters that are common to all the categories of devices that you have selected.
- Device Category-specific Parameters—This group of fields is specific to a device category. If, for a specified device category, only the common parameters are applicable, this message appears in the user interface:

  ```
  No Category-specific Commands
  ```

- Applicable Devices—This link is available in the device category-specific group of fields and enables you to view the devices in your selection, to which the device-specific parameters apply.
- Buttons in the system-defined tasks interface:

Button	Action
Save	Saves the information that you have entered in the fields in the task dialog box.
Reset	Clears all the fields.
Cancel	Cancels your changes, and closes the task dialog box.

For the cable devices, you can apply a task only to a single device at a time, because cable templates configure interfaces on devices.

Also, for the cable tasks to work correctly, you must have valid SNMP credentials in Device and Credential Repository (DCR). See *Administration of Cisco Prime LAN Management Solution 4.1* for more information on setting valid SNMP credentials.

Therefore, if you have selected more than one cable device and selected tasks for them, the task may not appear in the Applicable Tasks pane of the Add Tasks dialog box. For the tasks that are applicable to cable devices, see Table 4-5.

Understanding the NetConfig Credentials Configuration Tasks

NetConfig provides for tasks to configure credentials on devices. These tasks are:

- Enable Password (See Enable Password Task.)
- Local Username (See Local Username Task.)

- Radius Server (See RADIUS Server Configuration Task.)
- TACACS TACACS Configuration Task
- TACACS+ (See TACACS+ Configuration Task.)
- SNMP Community (See SNMP Community Configuration Task.)
- SNMP Security (See SNMP Security Configuration Task.)

The credential store allows only one set of login credentials per device - Primary username and primary password, irrespective of the authentication type.

Hence, this imposes certain limitations on the NetConfig templates, especially, when you are configuring/modifying the authentication method on the device.

To overcome this, an option to specifically update the credential store is provided in the credential tasks. The credential store is updated only when this option is chosen with the values specified.

The usage of NetConfig credentials tasks to configure the credentials on a device should be based on the active credentials (e.g. Telnet, TACACS, etc.) in the device. For example if the device is configured with TACACS+, you should use only TACACS+ template to configure the credentials.

Example

When you remove the TACACS+ authentication for the device, the device reverts to the authentication method that was earlier configured on it. For example, the local username.

However, LMS is unaware of the fallback authentication method, and the respective credentials. If Device and Credential Repository is not updated with the right credentials, the subsequent device operations from LMS will fail.

In this case, you should select the option to update the local credential store and specify the local username credentials. When the job runs, NetConfig updates Device and Credential Repository with this set of credentials, so that for subsequent devices, access from LMS will be successful.

Adhoc Task

You can use the Adhoc system-defined task to add configuration commands to a job, during job definition.

You cannot save an instance of an Adhoc task, for future use. If you need to reuse a template that provides capabilities unavailable from the system-defined tasks, you can create a user-defined tasks (see Creating and Editing User-defined Tasks).

Caution NetConfig does not validate commands you enter in the Adhoc task. If you enter incorrect commands, you might misconfigure or disable devices on which jobs that use the task run.

Groups for each of the device categories that you have selected, appear in the Adhoc Configuration dialog box. To invoke the Adhoc Configuration dialog box, see Starting a New NetConfig Job.

You can enter configuration and rollback commands for these device categories:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS

- NAM
- PIX OS

For more details, see Table 4-5.

Note As Cable devices fall under the IOS category, you can enter adhoc commands in the IOS group of fields in the Adhoc Configuration dialog box.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Adhoc Configuration dialog box are:

Group	Field	Description
Commands	CLI Command	Enter configuration commands. You can also enter interactive commands (see Handling Interactive Commands) and multi-line commands see Handling Multi-line Commands).
	Rollback Command	Enter rollback commands.
Command Mode	Config or Enable	Select the mode (config or enable) in which the task configuration commands will run. If you have selected Catalyst OS, or NAM devices, then the enable mode is preselected, and you do not have the option to select the config mode. The Command Mode group is not available for the Adhoc Task selected in the Port Based flow of the NetConfig job.

If you enter any credential command in the CLI Commands or Rollback Commands fields, then those credentials will be masked in the job work order and the job results page.

For example, the command, `snmp-server community public ro` will be displayed as `snmp-server community ***** ro`.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Authentication Proxy Task

The Authentication Proxy feature helps users to log into the network or access the Internet using HTTP. Their specific profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS, or TACACS+ authentication server.

The Cisco Secure Integrated Software authentication proxy feature allows network administrators to apply specific security policies on a user to user basis. You can use the Authentication Proxy system-defined configuration Task on IOS devices, which have been configured for VPN functionality.

The IOS category of devices (including Cable devices) are supported by this task.

For more details, see Table 4-5.

You can enter the details of this task in the Authentication Proxy Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Authentication Proxy Configuration dialog box are:

Group	Sub-Group	Field	Description
IOS Parameters	Authorization (AAA)	Action	Select the required option to enable, disable or make no change to the authorization configuration.
		Method 1	Select either TACACS+ or RADIUS as your first method of authorization.
		Method 2	Select either TACACS+ or RADIUS as your second method of authorization, based on your selection in the first method
	Cache Timeout	Minutes (1-2147483647)	Timeout value. The default timeout value can be in the range of 1 and 2,147,483,647.
		Set to default	Select this to set the default cache timeout value of 60 seconds.
	Banner	Action	Select **Enable** or **Disable** to set or reset Banner display in the login page. • If you select **Enable**, the router name is displayed in the login page. • If you select **Disable**, then the router name is not displayed. If you do not want to make any changes to the banner, select **No Change.**
		Banner Text (Optional)	Enter the text that you want displayed in the banner. If you enter the banner text, then this text is displayed instead of the router name in the login page. This is an optional field.
	Authentication Proxy Rule	Action	Select **Enable** or **Disable** an authentication proxy rule. • If you select **Enable**, a named authentication proxy rule is created and associated with access list. • If you select **Disable**, the associated proxy rule is removed. Select **No Change** if you do not want to make changes to the Authentication Proxy Rule group of fields.
		Name	Enter a name for the authentication proxy rule. The name can be up to 16 alphanumeric characters.
		Overriding Timeout [optional(1-2147483647)]:	Enter a timeout value to override the default cache timeout. This is an optional field. The overriding timeout value should be in the range of 1 and 2,147,483,647.

Group	Sub-Group	Field	Description
		ACL Number/Name [optional]:	Enter a Standard Access list to be used with the Authentication proxy. This is an optional field.
	New Model	Action	Select to enable, disable, or make no change to new model state.

Click on **Applicable Devices** to view the devices in your selection, to which this task applies.

IOS Devices with VPN Images

You can determine VPN images from the naming convention used for IOS images. The naming convention follows the *xxxx-yyyy-ww* format.

Where, *xxxx* represents platform, *yyyy* represents features and ww represents format. If the middle value (*yyyy*) contains, the number `56` or `k`*n*, where *n* is a number between 1 and 9, then this is a VPN image.

For example, `C7100-IS56I-M` is a VPN image, since it contains the number `56`.

Banner Task

You can use the Banner system-defined, configuration task to change banners on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS

For more details, see Table 4-5.

You can enter the details of this task in the Banner Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Banner Configuration dialog box are:

Group	Sub Group	Field	Description
Common Parameters	Motd Banner	Action	Select the appropriate option to add or remove a message of the day banner. Select **No Change**, if you are modifying an existing task, and you do not want to change the value in this field.
		Message	Enter message, if you selected **Add** in Action field.
IOS Parameters	Exec Banner	Action	Select the appropriate option to add or remove an Exec banner. Select **No Change**, if you are modifying an existing task, and you do not want to change the value in this field.
		Message	Enter message, if you selected **Add** in Action field.
	Incoming Banner	Action	Select the appropriate option to add or remove an Incoming banner. Select **No Change**, if you are modifying an existing task, and you do not want to change the value in this field.

Group	Sub Group	Field	Description
		Message	Enter message, if you selected **Add** in Action field.
	Login Banner	Action	Select the appropriate option to add or remove a Login banner. Select **No Change**, if you are modifying an existing task, and you do not want to change the value in this field.
		Message	Enter message, if you selected **Add** in Action field.
	Slip-PPP Banner	Action	Select the appropriate option to add or remove a Slip/PPP banner. Select **No Change**, if you are modifying an existing task, and you do not want to change the value in this field.
		Message	Enter message, if you selected **Add** in Action field.
CatOS Parameters	No category-specific commands.	-	This device category does not have any device-category-specific commands. Use the Common Parameters group to assign the values.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

CDP Task

You can use the CDP system-defined task to configure Cisco Discovery Protocol (CDP) on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine

For more details, see Table 4-5.

You can enter the details of this task in the CDP Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the CDP Configuration dialog box are:

Group	Sub Group	Field	Description
Common Parameters	Run	Action	Select to enable, disable, or make no change to the CDP state.
	Hold Time	Seconds (10-255)	Enter holdtime in seconds. The CDP holdtime specifies how much time can pass between CDP messages from neighboring devices before the device is no longer considered connected and the neighboring entry is aged out. Value must be greater than value in Update Time field.
		Set to Default	Select this for the default hold time of 60 seconds

Group	Sub Group	Field	Description
	Update Time	Seconds (5-254)	Enter time between CDP updates, in seconds. Value must be less than value in Hold Time field.
		Set to Default	Select this for the default update time of 60 seconds
	CDP Version	Run	Select the CDP Version (CDPv1 or CDPv2. CDP version 2 is the default value. If you are modifying the CDP Task and you do not want to change this field, select No Change.
IOS Parameters	No category-specific commands.	-	This device category does not have any device-category-specific commands. Use the Common Parameters group to assign the values.
CatOS Parameters	Mod/Ports	Mod/Ports (Ex:2/1-12,3/5)	Enter modules and ports on which to enable or disable CDP. You can enter a single module and port or a range of ports, for example, 2/1-12,3/5-12.
		All mod/ports	Select to enable or disable CDP in all ports in all modules.
	CDP Format	Format	The options are: • No Change (Does not allow you to make any modifications to the specified CDP format.) • MAC • Other Select the required option.
CE Parameters	No category-specific commands.	-	This device category does not have any device-category-specific commands. Use the Common Parameters group to assign the values.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Certification Authority Task

You can use the Certification Authority (CA) system-defined configuration task to provide manageability and scalability for IP Security (IPSec) standards. The Certification Authority task can be used only on IOS devices configured for VPN functionality.

This task is applicable to IOS devices (including Cable devices).

For more details, see Table 4-5.

You can enter the details of this task in the Certification Authority Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For this task to work correctly, you must use a CLI-based protocol (Telnet or SSH) as the download protocol.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Certification Authority Configuration dialog box are:

Group	Sub-Group	Field	Description
IOS Parameters	Declare CA	Action	Select **Enable** or **Disable** to activate/deactivate Certification Authority (CA). • If you select **Enable** you can create or modify CA. • If you select **Disable**, you can delete the CA. Select **No Change**, to leave the CA Name unchanged.
		CA Name	Enter the CA name. This name is used to identify the certification authority to be configured. This name is the CA domain name.
	Enrollment URL	Action	• Select **Enable** to allow router to connect to the CA, using the URL specified in the Value field. • Select **Disable**, if you do not want to connect to the CA. • Select **No Change** to leave the Enrollment URL field unchanged.
		Value	Enter the URL of the CA. The URL should include any available non-standard cgi-bin script location.
	Enrollment Mode	Action	• Select **Enable** if the CA provides a Registration Authority (RA). • Select **Disable** to disable the specified LDAP Server. • Select **No Change** to leave the Enrollment Mode field unchanged.
		LDAP Server	Enter the LDAP server of the CA, if your CA system provides an RA. LDAP server contains the location of CRLs (certification revocation lists) and certificates.
	Enrollment Retry Period	Minutes [1- 60]	Enter the wait period between certification request retries. The wait period is between 1 to 60.
		Set to Default	Select this option to set the default wait period to 1 minute.
	Enrollment Retry Count	Number [1- 100]	Enter the certification request retry number. The retry number must be between 1 and 100.
		Set to Default	Select this option to set the default retry period to 1 minute.
	CRL Optional	Action	Select **Enable** to bypass the Certificate Revocation List. If you select **Disable**, Certificate Revocation list is checked.

Group	Sub-Group	Field	Description
	Certificate Query	Action	Select an option to enable, disable or make no change to certificate query. • If you select **Enable**, certificate query will be added to all trust points on the router. • If you select **Disable**, the certificate will not be queried.
	RSA Key pairs	Action	Select an option to generate, delete or make no change to the RSA key pairs. This feature allows you to configure a Cisco IOS router to have multiple key pairs. Thus, the Cisco IOS software can maintain a different key pair for each identity certificate.
		Key Type	Specify the key type: • General Purpose—To generate a general purpose key pair that is used for both encryption and signature. • Usage—To generate separate usage key pairs for encrypting and signing documents.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

IOS Devices with VPN Images

You can determine VPN images from the naming convention used for IOS images. The naming convention follows the *xxxx-yyyy-ww* format.

Where, *xxxx* represents platform, *yyyy* represents features and ww represents format. If the middle value (*yyyy*) contains, the number `56` or `Kn`, where *n* is a number between 1 and 9, then this is a VPN image.

For example, `C7100-IS56I-M` is a VPN image, since it contains the number `56`.

Crypto Map Task

You can use the Crypto Map Server system-defined task to configure IPSec on devices.

Note You must configure the IKE configuration system-defined task (see Internet Key Exchange (IKE) Configuration Task) and Transform system-defined task (see Transform System-Defined Task) before configuring the Crypto Map system-defined task.

The following device categories are supported by this task:

- IOS (including Cable devices)
- PIX OS

For more details, see Table 4-5.

You can enter the details of this task in the Crypto Map Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Crypto Map Configuration dialog box are:

Group	Sub-Group	Field	Descriptions
IOS Parameters	Configuration	Action	Select an option to add, remove, or make no change to the IOS configuration.
		Map Name	Enter the name for the Crypto Map.
		Map Number	Enter the number for the Crypto Map. The value must be between 1 and 65535.
		Map Type	Select the map type (manual or isakmp) for the Crypto Map.
		Map Description	Enter the description for the Crypto Map.
		Crypto ACL	Enter the extended access list for Crypto Map.
		IPSec Peer	Enter the IPSec peer to be associated with the Crypto Map.
		Transform Set name	Enter the transform set name to be used with the Crypto Map.
PIX Parameters	Configuration	Action	Select an option to add, remove, or make no change to the PIX configuration.
		Map Name	Enter the name for the Crypto Map.
		Map Number	Enter the number for the Crypto Map. Value must be between 1 and 65535.
		Map Type	Select the type (manual or isakmp) for the Crypto Map.
		Crypto ACL	Enter the extended access list for Crypto Map.
		IPSec Peer	Enter the IPSec peer to be associated with the Crypto Map.
		Transform Set name	Enter the transform set name to be used with the Crypto Map.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

DNS Task

You can use the DNS system-defined task to configure DNS (Domain Name Server) on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see Table 4-5.

You can enter the details of this task in the DNS Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the DNS Configuration dialog box are:

Group	Sub-Group	Field	Description
Common Parameters	DNS Server	Add	Enter the IP addresses of DNS name server(s) that you want to add. Separate multiple addresses with commas. If the device accepts only one DNS server, then the first address will be considered.
		Remove	Enter the IP addresses of DNS name server(s) that you want to remove. Separate multiple addresses with commas.
	Domain Name	Name	Enter the domain names to complete unqualified hostnames. If a device has a domain list enabled, it will be used to complete unqualified hostnames instead of the domain name. Separate multiple addresses with commas. If the device accepts only one domain name, then the first entry will be considered.
		Remove	Select this option to remove the domain names.
IOS Parameters		Domain Lookup	Select to enable or disable IP DNS-based hostname-to-address translation.
		CLNS NSAP	Select to enable or disable or make no change to the CLNS NSAP option. If this option is enabled, any packet with the specified CLNS NSAP prefix causes CLNS (Connectionless Network Service) protocol to behave as if no route were found.
		OSPF	Select to enable or disable or make no change to the OSPF (Open Shortest Path First) protocol option.
	Domain List	Action	Select an option to add, remove, or make no change to the domain list.
		Domain List	Enter domain names to complete unqualified hostnames, or add to the existing list. Separate multiple domain names with commas. Do not include an initial period before domain names.
CatOS Parameters		1st Server Primary	Select to have a DNS name server entered in Add field, as the default or the primary name server.
		Domain Lookup	Select an option to enable, disable, or make no change to the domain lookup.
Content Engine Parameters		Serial Lookup	Select an option to enable, disable, or make no change to the serial lookup.

Group	Sub-Group	Field	Description
CSS Parameters	Secondary DNS Server	Add (Hostname or IP Address)	Enter the hostname or an IP address of a secondary server, that you want to add. A maximum of two IP addresses are allowed. The order in which you enter them is the order in which they are used if the primary DNS server fails. Separate multiple addresses with a comma.
		Remove (Hostname or IP Address)	Enter a hostname or an IP address of a secondary server, that you want to remove. A maximum of two IP addresses are allowed. Separate multiple addresses with a comma
NAM Parameters		Disable Nameservers	Select to disable domain name servers.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Enable Password Task

You can use the Enable Password system-defined, configuration task to change the enable and secret passwords, which allow users to enter the enable mode on devices.

When you enable or disable an enable password, the change is made on the device and in Device and Credential Repository.

Note If you disable the enable password on a device, you cannot enter the enable mode on that device unless you previously enabled an alternative type of enable mode authentication.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- PIX OS

For more details, see Table 4-5.

You can enter the details of this task in the Enable Password Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Note If you change the enable password on a Catalyst device with an RSM module using this task, the RSM enable password is also changed.

The fields in the Enable Password Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Setup	Action	Select an option to enable, disable or make no change to the enable password.
		Password	Enter the enable password.
		Verify	Re-enter the password.
IOS Parameters	Password	Level (1-15)	Set the Enable Password level. The level can be between 1 and 15. 15 is the default level. For an IOS device, it is advisable not to disable both Enable Password and Enable Secret password. This is because the IOS device will not allow you to go into the Enable mode of the device. You can do this only if you have the console password for the device. If you have selected Enable Password as **No Change** in the Common Parameters pane, and selected Disable for Enable Secret in the IOS Parameters pane, then Enable Secret Password is updated in the Device and Credentials database. If you have selected Enable Password as **Disable** in the Common Parameters pane, and selected **No Change** for Enable Secret in the IOS Parameters pane, then Enable Password is updated in the Device and Credentials database.
		Encrypted	Select this option to encrypt the password.
		Update Credentials	Select this to update credentials. For details see Understanding the NetConfig Credentials Configuration Tasks
	Secret	Action	Select an option to enable, disable or make no change to the secret password.
		Secret	Enter the secret password.
		Verify	Re-enter the password.
		Level (1-15)	Set the password level. The level can be between 1 and 15. 15 is the default level.
		Encrypted	Select this option to encrypt the password.
CatOS Parameters	Password	Apply Command on Modules	Select to apply the command on the modules. If you have selected **Disable** as the action in the Common Parameters group, then the password will be removed.

Group	Sub-group	Field	Description
PIX Parameters		Level(0-15)	Set the password level. The level can be between 0 and 15. 15 is the default level.
		Encrypted (Password should be 16 characters)	Select this option if the password you are entering is already encrypted. If you select this option ensure that your password is 16 characters.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

HTTP Server Task

You can use HTTP Sever to configure HTTP access on IOS devices, which have been configured for VPN functionality.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS

For more details, see Table 4-5.

You can enter the details of this task in the HTTP Server Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the HTTP Server Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Server	Action	Select an option to enable, disable or make no change to the HTTP access on the device.
	Port	Number [0-65535]	Specify the HTTP server port number.
		Set to Default	Select this option to set the default port (80).
IOS Parameters	Authentication	Action	Select an option to enable, disable or make no change to the authentication method.
		Method	Select an authentication method: • AAA • enable • local • TACACS
	Access List	Action	Select an option to enable, disable or make no change to the access list.

Group	Sub-group	Field	Description
		ACL Number/Name	Enter the Access Control List number or name to be used. The access list number must be between 1 to 99.
CatOS Parameters			No category-specific commands.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

You will lose Telnet access to the device if you configure HTTP Server. The Device may require TACACS/RADIUS/Local username and password after configuring HTTP Server. You should make sure that the device has the appropriate login configured. The username and password has to be stored in the LMS Database.

IOS Devices with VPN Images

You can determine VPN images from the naming convention used for IOS images. The naming convention follows *xxxx-yyyy-ww* format.

Where, *xxxx* represents platform, *yyyy* represents features and ww represents format. If the middle value (*yyyy*) contains, the number `56` or `k`*n*, where *n* is a number between 1 and 9, then this is a VPN image.

For example, `C7100-IS56I-M` is a VPN image, since it contains the number `56`

Local Username Task

You can use the Local Username system-defined task configure local username and password authentication on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- CSS

For more details, see Table 4-5.

You can enter the details of this task in the Local Username Task Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Local Username Task Configuration dialog box are:

Group	Sub-Group	Field	Description
Common Parameters	Local User Setup	Action	Select an option to add, remove or make no change to the local username setup.
		Username	Enter the local username.
		Password	Enter local username password.
		Verify	Re-enter the password.

Group	Sub-Group	Field	Description
IOS Parameters	Local User Setup	Privilege Level [0-15]	Set the required privilege level.
Local User Setup		Privilege Level [0-15]	Set the required privilege level.
		No HangUp	Select this option to enable No Hang Up mode.
		No Escape	Select this option to enable No Escape mode.
Local User Login Authentication		Action	Select to enable, disable or make no change to the local user authentication group of fields.
	Local Username Credentials	Username	Values are entered in Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Password	Values are entered in Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Verify	Values are entered in Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.
CSS Parameters			For CSS devices: • The username length should be between 1 and 16 characters. • The local password length should be between 6 and 16 characters. • The DES-Encrypted password length should be between 6 and 64 characters.
Local User Setup		SuperUser	Select this option to designate the local user as superuser.
		Password Type	Select the password type from these options: • Local • Encrypted • DES_Encrypted
Directory Access		Configure Directory Access	Select this option if you want to configure directory access. Defines the CSS directory access levels. By default, CSS assigns users with read and write access to the directories. Changing the access level also affects the use of the CLI commands associated with the directories.
	Directories	Script	Select the required access option to the Script directory: • No Access • Read And Write • Read • Write

Group	Sub-Group	Field	Description
		Log	Select the required access option to the Log directory: • No Access • Read And Write • Read • Write
		Root	Select the required access option to the Root directory: • No Access • Read And Write • Read • Write
		Archive	Select the required access option to the Archive directory: • No Access • Read And Write • Read • Write
		Release Root	Select the required access option to the Release Root directory: • No Access • Read And Write • Read • Write
		Core	Select the required access option to the Core directory: • No Access • Read And Write • Read • Write
		MIB	Select the required access option to the MIB directory: • No Access • Read And Write • Read • Write

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

IGMP Configuration Task

You can use this task to configure the Internet Group Management Protocol (IGMP) on a cable interface.

Note You can apply this task only on a single IOS device at a time. For details, see Table 4-5.

You can enter the details of this task in the IGMP Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the IGMP Configuration dialog box are:

Group	Sub-group	Field	Description
IOS Parameters			
IGMP Configuration	Interface	Interfaces	Select the required option to specify the interface to be configured for IGMP, or to make no change to the existing interface selection: • Not Selected • FastEthernet0/0 • FastEthernet0/ • Cable1/0
		Action	Select the required option to enable, disable, or make no change to the Interface sub-group of fields.
		PIM Mode	Select the required PIM mode option. Select **No Change** to retain any previous mode selection: • No Change • dense-mode • sparse-mode • sparse-dense-mode
IGMP Parameters		Action	Select the required option to replace the values in, or to make no change to the IGMP Parameters group of fields.
		IGMP Version	Select the required IGMP version from the supported versions: • 1 • 2 • 3
		Last Memory Query Interval [100-25500 in msec]	Enter the time interval between the IGMP specific messages sent by the router. Enter the last memory query interval in seconds. You can enter an interval between 100 and 25500 milliseconds. The default is 1000 milliseconds.

Group	Sub-group	Field	Description
		Query Maximum Response Time[1-25 in sec]	Enter the maximum response time advertised in the IGMP queries. This option is enabled when IGMP version 2 is configured. You can enter a response time between 1 and 25 seconds. The default is 10 seconds.
		Query Interval [1-65535 in sec]	Indicates a time interval when the Cisco IOS software sends IGMP host queries. Enter a query interval between 1 and 65535 seconds. The default is 60 seconds.
		Query Timeout [60-300 in sec]	Indicates the timeout period when the router takes the query of an interface after the previous query has stopped querying. You can enter a value between 60 and 300 seconds. The default is 2* Query Interval second.
		Helper Address (Should be in IP address format)	Indicates the IP address that will receive all IGMP host reports, and also where you can leave messages. This option is enabled when IGMP version 2 is configured. Enter the Helper Address in the IP Address format.
Group Configuration		Action	Select the required option to add values to, or to make no change to the Group Configuration group of fields.
		ACL to control joining of Multicast Group	Allows you to control the multicast groups. You can enter either the IP access list name or number. The valid range is between 1 and 99.
		Join Group Multicast Address (multiple addresses should be separated by commas)	Adds Join Group Multicast Address to the Multicast Address table. Enter the addresses, separated by commas.
		Static Group Multicast Address (multiple addresses should be separated by comma)	Adds Static Group Multicast Address to the Multicast Address table. Enter the addresses, separated by commas.
		Populate for all Groups	Allows you to apply the configuration to all groups.

Click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Interface IP Address Configuration Task

You can use this task to configure the IP address of a cable interface.

Note You can apply this task only on a single IOS device at a time. For details, see Table 4-5.

You can enter the details of this task in the Interface IP Address Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Interface IP Address Configuration dialog box are:

Group	Sub-group	Field	Description
Cable Parameters			
Interface IP Configuration		Cable Interface	Select the required cable interface for configuring the IP address, or select **Not Selected** to make no change to the previous selection: • Not Selected • FastEthernet0/0 • FastEthernet0/1 • Cable1/0
		Action	Select the following action: • No Change—Makes no change to the IP Addresses • Replace—Replaces the IP Addresses • Remove Primary—Removes the primary IP Address. • Remove Secondary—Removes the secondary IP Address. • Remove All—Removes both primary and secondary IP Addresses.
	IPAddress	Primary	Enter the primary IP address.
		Secondary	Enter the secondary IP address.
	Subnet Mask	Primary	Enter the primary subnet mask.
		Secondary	Enter the secondary subnet mask.

Note The values for interfaces are as returned by device.

Click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Internet Key Exchange (IKE) Configuration Task

Use the Internet Key Exchange (IKE) Configuration System task to configure IPSec on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- PIX OS

For more details, see Table 4-5.

You can enter the details of this task in the IKE Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Group	Sub-group	Field	Description
IOS Parameters			
ISAKMP		Action	Select to enable, disable, or make no change to ISAKMP.
ISAKMP Policy	ISAKMP Policy Priority	Action	Select to add, remove, or make no change to ISAKMP policy priority.
		Priority [1-10000]	Enter the policy priority number Value must be between 1 and 10000.
	Encryption	Action	Select to enable, disable, or make no change to encryption type.
		Type	Select the type of encryption for the policy: • 3des • des
	Hash	Action	Select to enable, disable, or make no change to the hash algorithm.
		Algorithm	Select the type of hash algorithm: • sha • md5
	Authentication	Action	Select to enable, disable, or make no change to the authentication method.
		Method	Select the type of authentication method: • rsa-sig • rsa-encr • pre-share
	Group	Action	Select to enable, disable, or make no change to the Diffie-Hellman group identifier.
		Value	Enter the Diffie-Hellman group identifier. Value must be 1 or 2.
	Lifetime	Action	Select to enable, disable, or make no change to the lifetime value.
		Seconds [60-86400]	Enter the lifetime value in seconds. Value must be between 60 and 86400 seconds.
PIX Parameters			
ISAKMP		Action	Select to enable, disable, or make no change to ISAKMP.
		Interface	Select the interface: • Inside • Outside
ISAKMP Policy	ISAKMP Policy Priority	Action	Select to add, remove, or make no change to ISAKMP policy priority.

Group	Sub-group	Field	Description
		Priority [1-65534]	Enter the policy priority number Value must be between 1 and 10000.
	Encryption	Action	Select to enable, disable, or make no change to encryption type.
		Type:	Select the type of encryption: • aes • aes-192 • aes-256 • des • 3des
	Hash	Action	Select to enable, disable, or make no change to the hash algorithm.
		Algorithm	Select type of hash algorithm: • sha • md5
	Authentication	Action	Select to enable, disable, or make no change to the authentication method.
		Method	Select the type of authentication method: • rsa-sig • pre-share
	Group	Action	Select to enable, disable, or make no change to the Diffie-Hellman group identifier.
		Value	Enter the Diffie-Hellman group identifier. Value must be 1, 2 or 5.
	Lifetime	Action	Select to enable, disable, or make no change to the lifetime value.
		Seconds [120-86400]	Enter the lifetime in seconds. Value must be between 120 and 86400 seconds.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

NTP Server Configuration Task

You can use the NTP Server system-defined task to configure Network Time Protocol (NTP) on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- CSS
- CE

For more details, see Table 4-5.

You can enter the details of this task in the NTP Server Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Group	Sub-group	Field	Description
Common Parameters	NTP Server	Action	Select to add, remove, or make no change to Network Time Protocol.
		Host Name/IP Address	Enter the IP address of the NTP server to which devices will send time-of day requests.
IOS Parameters	NTP Server	Server Type	Select the required server type.
		Version	Select the server version.
		Server Key (0-4294967295)	Enter the NTP server Key. The value must be between 0 and 4294967295.
		Verify Server Key	Re-enter the Key to confirm.
		Source Interface (Interface Name)	Enter the source interface name.
		Preferred	Select an option to specify whether the interface is a preferred interface.
	NTP Authentication Key	Action	Select to add, remove, or make no change to the NTP authentication Key.
		Number [1 to 4294967295]	Enter the number of Key bits. The value must be between 1 and 4294967295 Key bits.
		Verify Number	Re-enter the number to confirm.
		MD5 Number (Max 8 chars)	Enter the MD5 number which can contain a maximum of 8 characters.
	NTP Authentication	NTP Authentication	Select to enable, disable, or make no change to NTP authentication.
	NTP Calendar	Action	Select to add, remove, or make no change to the NTP calendar.
	NTP Access Group	Action	Select to add, remove, or make no change to the NTP access group.
		Access Type	Select the required action type: • QueryOnly • ServeOnly • Serve • Peer
		ACL Number [1-99]	Enter the ACL number which should be a value between 1 and 99.
	NTP Trusted Key	Action	Select to add, remove, or make no change to the NTP trusted Key.

Group	Sub-group	Field	Description
		Key Number [1-4294967295]	Enter the Key number whcih must be a value between 1 and 4294967295.
		Verify Key Number	Re-enter the Key number to verify.
CatOS Parameters	NTP Server	Server Key [Range:1 to 4292945295]	Enter the NTP server Key which must be between 1 to 4292945295.
		Verify Server Key	Re-enter the Key to confirm.
	NTP Client	Client Action	Select to enable, disable, or make no change to NTP client.
	NTP Authentication	NTP Authentication	Select to enable, disable, or make no change to NTP authentication.
	NTP Key	Action	Select to add, remove, or make no change to the NTP Key.
		Key Number [1 to 4292945295]	Enter the NTP server Key and the value must be between 1 to 4292945295.
		Verify Key Number	Re-enter the Key to confirm.
		Type	Select the required Key type.
		MD5 Number [Max 32 chars]	Enter the MD5 number which should be a maximum of 32 characters.
CE Parameters	NTP Server	Action	Select to enable, disable, or make no change to the NTP server.
		Server Type	Select the required server type.
CSS Parameters		NTP Server Version	Select the required NTP server version.
	NTP Server Poll Interval	Action	Select to add, remove, or make no change to the NTP poll interval.
		Poll Interval [16-16284 seconds]	Specify the poll interval. The value must be between 16 and 16284 seconds.

RADIUS Server Configuration Task

You can you use the RADIUS system-defined task to configure RADIUS on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- CSS
- CE

For more details, see Table 4-5.

You can enter the details of this task in the RADIUS Server Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Group	Sub-group	Field	Description
Common Parameters			
Host Configuration		Action	Select to enable, disable, or make no change to the server configuration.
		Server Name	Enter the server name.
		Auth Port (0-65536)	Enter port used for authentication by RADIUS server.
Key Configuration		Action	Select to enable, disable, or make no change to the key configuration.
		Key	Enter RADIUS authentication and encryption key string used by server specified in Host area.
		Verify	Re-enter RADIUS key.
Login Authentication		Action	Select to enable, disable, or make no change to the login authentication. The Login Authentication is not applicable for CSS
	RADIUS Credentials	Username	Enter the username. For details see Understanding the NetConfig Credentials Configuration Tasks. In case of CSS devices, this value will be used to update the Primary login details.
		Password	Enter the password. For details see Understanding the NetConfig Credentials Configuration Tasks. In case of CSS devices, this value will be used to update the Primary login details.
		Verify	Re-enter the password to verify. For details see Understanding the NetConfig Credentials Configuration Tasks. In case of CSS devices, this value will be used to update the Primary login details.
IOS Parameters			
Login Authentication	List	Name	Enter default or named list.
		Set to Default	Select to set the default list.
	Type	Options (Drop-down list 1)	Select the required option: • No Choice • radius • tacacs+ • line • enable • local • none Similarly, select the type from the other three drop-down lists.

Group	Sub-group	Field	Description
New Model		Action	Select to enable, disable, or make no change to new model state.
Enable mode Authentication		Action	Select to add, remove, or make no change to the enable mode authentication.
	Credentials	Username	Enter the enable username.
		Password	Enter the enable password.
		Verify	Re-enter the enable password.
	Type	Options (Drop-down list 1)	Select the required option: • No Choice • radius • tacacs+ • line • enable • local • none Similarly, select the type from the other three drop-down lists.
Content Engine Parameters			No category-specific commands.
CSS Parameters	Host Configuration	Action	Select to enable, disable, or make no change to the host configuration.
		Secondary Server Name (Host Name or IP Address)	Enter the secondary server hostname or IP address.
		Secondary Server Key	Enter the key for the secondary server. Defines the secret string for authentication transactions between the RADIUS server and the CSS. Enter a case-sensitive string with a maximum of 16 characters.
		Verify	Re-enter the key to verify.
		Authentication Port (1-65535)	Enter custom authentication port of the RADIUS server. Value must be between 0 and 65535. Optional field. Defines the UDP port on the secondary RADIUS server that receives authentication packets from clients. Enter a number from 0 to 65535. The default is 1645.
Other Parameters		Dead Time in seconds (1-255)	Enter the dead time in seconds. The value must be between 0 and 255. Enter a number from 0 to 255. The default is 5. If you enter 0, the dead time is disabled and the CSS does not send probe access-request packets to the non-responsive server. This command applies to primary and secondary servers.
		Remove	Select to remove the dead time specification. Use the `no` form of this command to reset the dead-time period to its default of 5 seconds.

Group	Sub-group	Field	Description
		Retransmit (1-30)	Enter the retransmit value (between 1 and 30) number of times that the CSS retransmits an authentication request. Enter a number from 1 to 30. The default number is 3.
		Remove	Use the `no` form of this command to reset the retransmission of authentication request to its default of 3.
		Source Interface Host (Host Name or IP Address)	Enter the source interface hostname or IP address. Source Interface Host configuration is required to accept authentication from the RADIUS client. Note that this IP interface address is used for the NAS-IP-Address RADIUS attribute in the RADIUS Authentication Request.
		Remove	Select to remove the source interface specification.
		Timeout (1-255):	Enter the timeout value (between 1 and 2555). Timeout specifies the period of which the CSS waits for a reply to a RADIUS request before retransmitting requests to the RADIUS server.
		Remove	Select the remove option to reset the interval to its default of 10 seconds.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

RCP Configuration Task

You can use the RCP system-defined configuration task to configure RCP on devices.

This task supports the IOS category of devices including Cable devices.

For more details, see Table 4-5.

You can enter the details of this task in the RCP Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box)

The fields in the RCP Configuration dialog box are:

Group	Sub-group	Field	Description
IOS Parameters	Enable	Action	Select to enable or disable rcp state. To make rcp setup changes without enabling or disabling rcp, select **No Change**.
	RCP User Setup	Action	Select the required option to add to, or to remove current user from rcp authentication list. To make rcp setup changes without enabling or disabling rcp, select **No Change**.
		Local Username	Enter local name of user whose rcp access you are modifying.
		Remote Host	Enter IP address of remote host from which local device will accept remotely executed commands.

		Remote Username	Enter username on remote host from which device will accept remote commands.
		Enable Mode Commands	Click to allow remote user to run enable commands using rsh or to copy files to device using rcp.
		add/remove	Click **Add** to add current user to rcp authentication list. Click **Remove** to remove current user from rcp authentication list.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Reload Task

You can use the Reload task to schedule reload of devices. This task supports the IOS, Cat OS, SFS, NAM, CE, FastSwitch, PIX, CSS and Cable categories of devices. For more details, see Table 4-5.

You can enter the details of this task in the Reload Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box)

The fields in the Reload Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Reload	Action	Select either: • **Reload** to enable reloading selected devices. or • **No Change** if you do not want to schedule a reload for the selected devices.
IOS Parameters	Do not Save config before reload	Action	You can: • Check this option if you do not want to save the configurations before reloading. or • Uncheck this option if you want to save the configurations before reloading.
CatOS Parameters			No category-specific parameters.
CE Parameters	Do not Save config before reload	Action	You can: • Check this option if you do not want to save the configurations before reloading. or • Uncheck this option if you want to save the configurations before reloading.

NAM Parameters	Do not Save config before reload	Action	You can: • Check this option if you do not want to save the configurations before reloading. or • Uncheck this option if you want to save the configurations before reloading.
SFS Parameters			No category-specific parameters.
Fast Switch parameters			No category-specific parameters.
PIX Parameters	Do not Save config before reload	Action	You can: • Check this option if you do not want to save the configurations before reloading. or • Uncheck this option if you want to save the configurations before reloading.
CSS Parameters			No category-specific parameters.
Cable Parameters	Do not Save config before reload	Action	You can: • Check this option if you do not want to save the configurations before reloading. or • Uncheck this option if you want to save the configurations before reloading.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which the reload task applies.

SNMP Community Configuration Task

You can use the SNMP Community Configuration system-defined task to replace, add, and remove device SNMP community strings.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see Table 4-5.

You can enter the details of this task in the SNMP Community Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the SNMP Community Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Read-only	Action	Select an option to replace, add, remove, or make no change to a read-only SNMP community string. • If you select **Replace**, the new community string replaces the corresponding community string in the Device and Credential Repository (DCR). This action also deletes the current SNMP credentials on the device. • If you select the **Add** or **Remove** option, the new SNMP community strings are configured in the device alone and DCR is untouched. However if you select **Replace**, then the new SNMP community strings replace the community strings in the device as well as in DCR. If you select **No Change**, no change will be made to the Read-only Community string.
		Community String	Enter the community string.
		Verify	Re-enter the community string.
	Read-write	Action	Select an option to replace, add, remove, or make no change to a read-write SNMP community string. • If you select **Replace**, the new community string replaces the corresponding community string in the Device and Credential Repository. • If you select **Add** or **Remove**, the new SNMP community strings are configured in the device alone and DCR is untouched. However if you select **Replace**, then the new SNMP community strings replace the community strings in the device as well as in DCR. If you select **No Change**, no change will be made to the Read-write Community string.
		Community String	Enter the community string.
		Verify	Re-enter the community string.
IOS Parameters	Setup View (Optional)	MIB View (Optional)	Enter name of a previously defined view that defines objects available to community. Optional field.
		OID -Tree	Indicates the Object Identifier of ASN.1 subtree that is to be included or excluded from the view. To identify an Object Identifier ASN.1 subtree, enter a numerical string such as 1.3.6.2.4 or a word such as system. To identify a subtree family, enter a wildcard, for example an asterisk (*), where the string will read 1.3.*.4. Enter the MIB OID-Tree name.

Group	Sub-group	Field	Description
		Type	Include or exclude all the objects specified in the MIB OID subtree you identified in the previous field. Select **Included** or **Excluded** from the drop down list.
	Access List (Optional)	Access List (Optional)	Enter an integer from 1 to 99 to specify a named or numbered access list of IP addresses that are allowed to use the community string to access SNMP agent. Optional field.
CatOS Parameters			No category-specific parameters.
CE Parameters			No category-specific parameters.
PIX Parameters			No category-specific parameters.
CSS Parameters			No category-specific parameters.
NAM Parameters			No category-specific parameters.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

SNMP Security Configuration Task

You can use this task to configure the SNMP Security feature on the following device categories:

- IOS (including Cable devices)
- Content Engine

For more details, see Table 4-5.

You can enter the details of this task in the SNMP Security Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the SNMP Security Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters		Action	Select an option, to add, remove, or make no change to the common parameters.
		(Drop-down list)	Select the required option for SNMP Groups/Users: • Group & Users • Group • Users When you select the Group option while adding task instances for this task, the user fields will not be disabled. This is because NetConfig needs the user information for configuring SNMP group commands in Catalyst OS devices.
		Group Name	Enter the group name. Indicates the SNMP Group in the SNMP protocol context.
		SNMP Versions	Select the SNMP version. SNMP version 1 and version 2 have No Auth and No Privacy. Version 3 has all levels of security.
	Users * - The entries in the first row will be updated in Device and Credential Repository	User Names Authen Pswds Authen Algorithm Privacy Paswds	• Username—Indicates the name of the user in the SNMPv3 protocol. • Authenticating Passwords—Indicates that the user is part of the group that is assigned Auth No Privacy or Auth Privacy security level. • Authenticating Algorithm—Indicates the authenticating algorithm is assigned to a group with Auth No Privacy or Auth Privacy security levels. • Privacy passwords—Indicates user is part of a group assigned Auth Privacy level of security. You can specify up to five usernames, for which you can enter authentication passwords, select the authentication algorithm, and specify the privacy passwords.
	Config Access Control [optional]		This section allows you to configure access options for an SNMP group.
		Read View	Specify the read view. This view is for users assigned to a specified group. Indicates an alphanumeric label, not exceeding 64 characters, for the SNMP view entry you are creating or updating.
		Write View	Specify the write view. Allows all users in the specified group to add, modify, or create a configuration.
		Notify View	Specify the notify view. This view notifies all the users in the specified group.
IOS Parameters	Access Control (optional)	Access List [1-99]	Enter the number of an Access List (1 and 99).

Group	Sub-group	Field	Description
	Engine ID [optional]	Action	Select to add, remove, or make no change to the engine configuration. SNMP Engine ID is an identification name for the local or remote SNMP engine.
		Type	Select the type of engine: • Local—Local SNMP server engine. • Remote—Remote SNMP server engine.
		ID	Enter the Engine ID (identification name for the local or remote SNMP engine).
		Remote host	Enter the hostname or IP address of the remote SNMP entity to which the user belongs.
Content Engine Parameters		Remote Engine ID [Optional]	Enter the remote engine ID. This is an optional field.

The SNMP Security template enables you to configure Groups as well as Users with certain privileges. These Groups can be rolled back but the Users cannot be rolled back.

This is because the User details will not be available in the running configuration. Since NetConfig uses the running config to do roll back, rolling back Users is not possible.You should run a separate job to remove or add Users as required.

For each device category, click on **Applicable Devices** to view the devices in your selection.

SNMP Traps Configuration Task

You can use this task to configure the host, trap notification, and trap/inform parameters. You can specify security parameters to communicate securely with the SNMP host. See SNMP Security Configuration Task to configure the SNMP security.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM

For more details, see Table 4-5.

You can enter the details of this task in the SNMP Traps Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the SNMP Traps Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Traps Notification	Action	Select to enable, disable, or make no change to the traps notification configuration. If you select **Enable**, the server will receive SNMP traps. If you select **Disable** the server will not receive any SNMP traps.
IOS Parameters			
Traps Notification Options	Type	Environmental	Select to send only environmental traps to the host.
		SNMP	Select to send the SNMP traps to the host.
Host Configuration		Action	Select to add, remove, or make no change to the host configuration.
		Username	Specifies the user name that is used for authentication. This field is available when No Authentication, Authentication or Privacy are selected.
		Host	Enter the hostname or IP address.
		SNMP Security	Select the SNMP security method: • SecureV2c • NoAuthenticationV3 • AuthenticationV3 • PrivacyV3 • None
		Notification Type	Select the notification type: • Trap • Inform
		UDP Port [0-65535]	Indicates the port that will receive the SNMP requests. The range for a valid port number between 0 and 65535. The default is 162.
	Community String	String	Enter the community string.
		Verify	Re-enter the community string to confirm.
	Direct Traps To Host	Environmental	Select to send only environmental traps to the host.
		SNMP	Select to send the SNMP traps to the host.
Trap/Inform Configuration	Traps Message	Action	Select to change, replace, disable or make no change to the trap configuration.
		Trap Timeout [1-1000 s]:	Specify the trap timeout value. This value must be between 1 and 1000 seconds.

Group	Sub-group	Field	Description
		Trap Queue Length [1-1000 events]:	Specify the trap queue length. The number of events that you specify must be between 1 and 1000.
	Inform Request	Action	Select to replace, disable, or make no change to the inform request.
		Inform Retries [0-100]	Enter the inform retires. The value should be between 0 and 100.
		Inform Timeout [0-4294967295]	Specify the inform timeout value. This value must be between 0 and 4294967295.
		Inform Pending [0-4294967295]	Specify the inform pending value. This value must be between 0 and 4294967295.
CatOS Parameters	Host Configuration	Action	Select to add, remove, or make no change to the host configuration.
		Host	Enter the hostname or IP address.
		Community String	Enter the community string.
		Verify	Re-enter the community string to confirm.
ContentEngine Parameters	Host Configuration	Action	Select to add, remove, or make no change to the host configuration.
		Host	Enter the hostname or IP address.
		Community String	Enter the community string.
		Verify	Re-enter the community string to confirm.
		SNMP Security	Select the SNMP security method.
PIX Parameters	Host Configuration	Action	Select to add, remove, or make no change to the host configuration.
		Host	Specify an IP address of the SNMP management station to which traps should be sent and/or from which the SNMP requests come. You can specify up to five SNMP management stations.
		Interface	Select the interface: • Inside [default] • Outside
		Notification Type	Select the notification type: • Trap & Poll [default]—Allows both traps and polls to be acted upon. • Trap—Only traps will be sent. This host will not be allowed to poll. • Poll—Traps will not be sent. This host will be allowed to poll.

Group	Sub-group	Field	Description
CSS Parameters		Action	Select to add, remove, or make no change to the parameters such as host name or IP address, trap community, source IP address in traps, specific host, trap type, and event.
		Host Name or IP Address	Enter the hostname or IP address of an SNMP host that has been configured to receive traps. A maximum of 5 hosts can be configured.
		Trap Community	Enter the trap community string/name to be used when sending traps to the specified SNMP host. Enter an unquoted text string with no spaces and with maximum length of 12 characters.
		Verify	Re-enter the trap community string to confirm.
		Source IP Address in Traps	Select the source IP address in traps. To set the source IP address in the traps generated by CSS select one of these options: • Egress Port—Obtains the source IP address for the SNMP traps from the VLAN circuit IP address configured on the egress port used to send the trap. You do not need to enter an IP address because the address is determined dynamically by the CSS. • Management—Places the management port IP address in the source IP field of the trap. This is the default setting. • Specific Host—Allows the user to enter the IP address to be used in the, source IP field of the traps. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) in the Specific Host field (the next field). • No Change (No change will be made to the source IP address if you select this option.)
		Specific Host	In the previous field, that is, Source IP Address in Traps, if you have selected the Specific Host option, then specify the IP Address of the specific host in this field.
		Trap Type	Select the trap type: • No Change (No change will be made to the trap type if you select this option). • Enterprise—When you use this keyword alone, it enables enterprise traps. You must enable enterprise traps before you configure an enterprise trap option. • Generic—The generic SNMP traps consist of cold start, warm start, link down, and link up.

Group	Sub-group	Field	Description
		Event	Select the event: • None • Module Transition • Power Supply Transition • Illegal Packet DOS attack • LAND DOS attack • Smurf DOS attack • SYN DOS attack • Lifetick message failure • Login Failure • System reload • Reporter state transitions • Service transition
NAM Syslog Host Configuration Parameters		Action	Select to add, remove, or make no change to the syslog host configuration.
		Index[1-65535]	Enter the syslog host index. The value should be between 1 and 65535.
		Host IP Address	Enter the host name or IP address.
		Community String	Enter the community string.
		Verify	Verify the community string.
		UDP Port[1-65535]	Enter the UDP port. The value should be between 1 and 65535.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Smart Call Home Task

You can use the Smart Call Home task to configure the LMS managed Cisco Catalyst 6500 devices with the Call Home feature.

You can enter the details for this task in the Smart Call Home Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

The fields in the Smart Call Home Configuration dialog box are:

Field/Button	Description
General Configuration	
Call Home Service	Select any of these: • **Enable** — Enables Smart Call Home service. • **Disable** — Disables Smart Call Home service. • **No Change** — No change is made to Smart Call Home Service.
Contact E-mail Addresses	
Action	Select any of these: • **Add** — Adds the contact e-mail addresses • **Remove** — Removes the contact e-mail addresses • **No Change** — The contact e-mail addresses is not changed. This is the default option.
Contact E-mail Address	Enter contact email address. You can enter one or more e-mail IDs. Each e-mail ID to be entered on a separate line.
E-mail Server	
Action	Select any of these: • **Add** — Adds one or more e-mail servers. You can add a maximum of five e-mail servers. • **Replace** — Adds new e-mail servers after removing all earlier e-mail servers. • **Remove** — Removes one or more e-mail servers • **No Change** —The e-mail servers are not changed. This is the default option.
E-mail Servers	Enter one or more e-mail servers. Enter each e-mail server on a separate line and specify priority for each of them. The priority can be between 1 and 100.
Sender From Email Address	
Action	Select any of these: • **Add** — Adds a sender e-mail address • **Remove** — Removes the sender e-mail address • **No Change** —The sender e-mail address is not changed. This is the default option.
Sender E-mail Address (from)	Enter the e-mail address from which the mail is sent.
Sender Reply-to Address	
Action	Select any of these: • **Add** — Adds a sender reply-to e-mail address • **Remove** — Removes the sender reply-to e-mail address • **No Change** —Not to change the sender reply-to e-mail address. This is the default option.
Sender Reply-to Address	Enter a sender reply to e-mail ID.

Field/Button	Description
Install Cisco Security Certificate	
Install Cisco Security Certificate	Check to install the HTTP certificate.
Profile Configuration	
Profile	Select either: • **CiscoTAC-1 Profile** Or • **Other Profiles**
Profile Name	Enter a profile name. This option is activated only if you have selected Other Profiles option in the Profile field.
Activate Profile	Select any of these: • **Enable** — Activates the selected profile. • **Disable** — Deactivates the selected profile. • **No Change** —Not to add or remove a profile. This is the default option
Transport Options	
Connect To	Select: • **Cisco.com** if you want to connect to Smart Call Home using Cisco.com • **Transport Gateway**, if you want to connect to Smart Call Home using a transport gateway. • **Other**, if you want to connect to Smart Call Home using transport option other than Cisco.com or Transport Gateway. CiscoTAC-1 profile does not support the Transport Gateway and Other option. So this option is not activated when you select CiscoTAC-1 profile.
Transport Details	
Transport Method	Select: • **No Change** — To make no change to the transport settings • **E-mail**— To use e-mail as the transport method. This option is selected if Transport Gateway is selected as the Connect to option and the HTTPS option is not activated. • **HTTPS** — To use HTTPS as the transport method.
E-mail Address	Enter the e-mail address, if you have selected E-mail as the transport method.
HTTPS URLs	Enter the HTTPS URL, if you have selected HTTPS as the transport method.
Alert Groups	
Inventory	Select any of the following: • **Enable** if you want to subscribe to the Inventory Alert Group. • **Disable** if you do not want to subscribe to the Inventory Alert Group. • **No Change** if you do not want to subscribe to or unsubscribe from Inventory Alert Groups. This is the default option. If you have selected CiscoTAC-1 Profile, you cannot change the Alert groups or Alert group settings. If you have selected Other Profiles, you can change the Alert groups and Alert group settings.

Field/Button	Description
Periodicity	Specify the periodicity for receiving these Inventory alerts. You can select: • **Asynchronous** — To receive the Inventory alerts on a specified day or time. In other words, not in a periodic manner. • **Daily** — To receive the Inventory alerts every day • **Weekly** — To receive the weekly consolidated Inventory alerts. • **Monthly**— To receive the monthly consolidated Inventory alerts
DOW	DOW refers to Date of Week. This list box is activated only if you select Weekly as the periodicity for receiving the Inventory alerts. Select any of the following days of the week: • **Sun** • **Mon** • **Tue** • **Wed** • **Thu** • **Fri** • **Sat** **Sun** is the default value. For example: Select **Tue** if you want to receive Inventory alerts every Tuesday.
DOM	DOM refers to Date of Month. This list box is activated only if you select **Monthly** as the periodicity for receiving the Inventory alerts. Select any value from **1** and **31** to receive Inventory alerts every month on the specified date. Day **1** is the default value. For example: Select **5**, if you want to receive Inventory alerts on the 5th day of every month.
Begin Time	Specify the date and time at which you want to receive the Inventory alerts. The format supported is *hh:mm*, where *hh* refers to hours and *mm* refers to minutes.
Configuration	Select any of the following: • **Enable** if you want to subscribe to the Configuration Alert Group. • **Disable** if you do not want to subscribe to the Configuration Alert Group. • **No Change** if you do not want to subscribe to or unsubscribe from Configuration Alert Groups. This is the default option. If you have selected CiscoTAC-1 Profile, you cannot change the Alert groups or Alert group settings. If you have selected Other Profiles, you can change the Alert groups and Alert group settings.

Field/Button	Description
Periodicity	Specify the periodicity for receiving these Configuration alerts. You can select: • **Asynchronous** — To receive the Configuration alerts on a specified day or time. In other words, not in a periodic manner. • **Daily** — To receive the Configuration alerts every day. • **Weekly** — To receive the weekly consolidated Configuration alerts. • **Monthly** — To receive the monthly consolidated Configuration alerts
DOW	DOW refers to Date of Week. This list box is activated only if you select Weekly as the periodicity for receiving the Configuration alerts. Select any of the following days of the week: • **Sun** • **Mon** • **Tue** • **Wed** • **Thu** • **Fri** • **Sat** **Sun** is the default value. For example: Select **Tue** if you want to receive Configuration alerts every Tuesday.
DOM	DOM refers to Date of Month. This list box is activated only if you select **Monthly** as the periodicity for receiving the Configuration alerts. Select any value from **1** and **31** to receive Configuration alerts every month on the specified date. Day **1** is the default value. For example: Select **5**, if you want to receive Inventory alerts on the 5th day of every month.
Begin Time	Specify the date and time at which you want to receive the Configuration alerts. The format supported is *hh:mm*, where *hh* refers to hours and *hh* refers to minutes.
Syslog	Select any of the following: • **Enable** if you want to subscribe to the Syslog Alert Group. • **Disable** if you do not want to subscribe to the Syslog Alert Group. • **No Change** if you do not want to subscribe to or unsubscribe from Syslog Alert Groups. This is the default option. If you have selected CiscoTAC-1 Profile, you cannot change the Alert groups or Alert group settings. If you have selected Other Profiles, you can change the Alert groups and Alert group settings.

Field/Button	Description
Severity	Select from any of these severities: • **catastrophic** • **disaster** • **fatal** • **critical** • **major** • **minor** • **warning** • **notification** • **normal** • **debugging** You will be notified when a syslog of the selected severity occurs.
Patterns	Specify a pattern of Syslogs for which you want to receive alerts.
Environment	Select any of the following: • **Enable** if you want to subscribe to the Environmental Alert Group. • **Disable** if you do not want to subscribe to the Environmental Alert Group. • **No Change** if you do not want to subscribe to or unsubscribe from Environment Alert Groups. This is the default option. If you have selected CiscoTAC-1 Profile, you cannot change the Alert groups or Alert group settings. If you have selected Other Profiles, you can change the Alert groups and Alert group settings.
Severity	Select from any of these severities: • **catastrophic** • **disaster** • **fatal** • **critical** • **major** • **minor** • **warning** • **notification** • **normal** • **debugging** You will be notified when an environment event of the selected severity occurs.

Field/Button	Description
Diagnostics	Select any of the following: • **Enable** if you want to subscribe to the Diagnostics Alert Group. • **Disable** if you do not want to subscribe to the Diagnostics Alert Group. • **No Change** if you do not want to subscribe to or unsubscribe from the Diagnostics Alert Groups. This is the default option. If you have selected CiscoTAC-1 Profile, you cannot change the Alert groups or Alert group settings. If you have selected Other Profiles, you can change the Alert groups and Alert group settings.
Severity	Select from any of these severities: • **catastrophic** • **disaster** • **fatal** • **critical** • **major** • **minor** • **warning** • **notification** • **normal** • **debugging** You will be notified when a diagnostics alert of the selected severity occurs.
Applicable Devices	Allows you to view the IOS devices in your selection.
Save	Saves the information you have specified.
Reset	Clears all fields and reverts to the default settings.
Cancel	Ignores your changes.

Syslog Task

You can use the Syslog system-defined task to configure the collection of syslog messages from devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see Table 4-5.

You can enter the details of this task in the Syslog Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Syslog Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Logging Host	Action	Select the required option to enable, disable, or make no change to list of hosts that receive syslog messages.
		Ex: host1.domain,host2,1.2.3.4:	Enter the IP addresses of hosts to be added to or removed from the list of hosts that receive syslog messages. Separate multiple addresses with commas.
IOS Parameters			
Logging On		Action	Select the required option to enable, disable, or make no change to syslog state. Select No Change to make syslog setup changes without enabling or disabling syslog logging.
Logging Facility		Action	Select the required option to enable, disable, or make no change to syslog logging facility.
		Parameter	Select the logging facility to which the syslog messages are logged.
Logging Level	Buffered	Action	Select the required option to enable, disable, or make no change to the buffered logging level.

Group	Sub-group	Field	Description
		Conditions	Select the required logging level from the drop-down list: • Default • alerts • critical • debugging • emergencies • errors • informational • notifications • warnings
	Console	Action	Select the required option to enable, disable, or make no change to the console logging level.
		Conditions	Select the required logging level from the drop-down list.
	Monitor	Action	Select the required option to enable, disable, or make no change to the monitor logging level.
		Conditions	Select the required logging level from the drop-down list.
	Trap	Action	Select the required option to enable, disable, or make no change to the trap logging level.
		Conditions	Select the required logging level from the drop-down list.
CatOS Parameters			
Console Logging On		Action	Select the required option to enable, disable, or make no change to console logging.
Server Logging On		Action	Select the required option to enable, disable, or make no change to server logging.
Logging Level		Action	Select the required option to enable, disable, or make no change to the logging level.
		Facility	Select the logging facility to which the syslog messages are logged.
		Level	Select the required logging level from the drop-down list.
Content Engine Parameters			
Logging On		Action	Select the required option to enable, disable, or make no change to logging.
Destination		Console	Select this option to specify the console as the logging destination.
		Disk	Select this option to specify the disk as the logging destination.
Logging Facility		Action	Select the required option to enable, disable, or make no change to syslog logging facility.
		Parameter	Select the logging facility to which the syslog messages are to be logged.

Group	Sub-group	Field	Description
Logging Priority	Console	Action	Select the required option to enable, disable, or make no change to the console logging priority.
		Conditions	Select the required logging priority from the drop-down list.
	Disk	Action	Select the required option to enable, disable, or make no change to the disk logging priority.
		Conditions	Select the required logging priority from the drop-down list.
	Host	Action	Select the required option to enable, disable, or make no change to the host logging priority.
		Conditions	Select the required logging priority from the drop-down list.
PIX Parameters		Time Stamp	Select the required option to enable, disable, or make no change to the time stamp specification.
		Logging On	
Logging Facility		Action	Select the required option to enable, disable, or make no change to syslog logging facility.
		Parameter	Select the logging facility to which the syslog messages are to be logged.
Message		Action	Select the required option to enable, disable, or make no change to the syslog message configuration.
		Syslog Message ID	Enter the syslog message ID.
		Conditions	Select the required logging level from the drop-down list.
Logging Level	Buffered	Clear Buffer	Select to clear the buffer.
		Action	Select the required option to enable, disable, or make no change to the buffered logging level.
		Conditions	Select the required logging level from the drop-down list.
	Console	Action	Select the required option to enable, disable, or make no change to the console logging level.
		Conditions	Select the required logging level from the drop-down list.
	Monitor	Action	Select the required option to enable, disable, or make no change to the monitor logging level.
		Conditions	Select the required logging level from the drop-down list.
	Trap	Action	Select the required option to enable, disable, or make no change to the trap logging level.
		Conditions	Select the required logging level from the drop-down list.
CSS Parameters		Facility	Select the logging facility to which to log syslog messages.
		Logging Level	Select the required logging level from the drop-down list.
		CLI Command	Select the required option to add, remove, or make no change to the CLI commands.
	Logging to Disk	Disk	Select the required option to add, remove, or make no change to the option of logging to disk.

Group	Sub-group	Field	Description
		Logfile Name	Enter the log file name.
		Buffer	Select the required option to add, remove, or make no change to the buffer configuration.
		Size [0-64000]	Enter the size of the buffer. Enter a value between 0 and 64000 bytes.
		To sys.log	Select the required option to add, remove, or make no change to the option of logging to a file called sys.log.
	Logging to Line	Line	Choose this option to send the log activity of a subsystem to an active CSS session.
		Active Session Name	Enter the name of the active session. Enter a case-sensitive unquoted text string with a maximum length of 32 characters.
	Logging to Mail	Send Mail	Select the required option to add, remove, or make no change to the e-mail option.
		Mail Address	Enter the e-mail IDs (comma separated).
		SMTP Host (Name or IP Address)	Enter the SMTP hostname or the IP address.
		Logging Level	Select the required logging level from the drop-down list.
		Domain Name (Optional)	Enter the domain name of the SMTP host. This is an optional field.
NAM Parameters	MIB Threshold	Local	Select the required option to enable, disable, or make no change to the local MIB threshold.
		Remote	Select the required option to enable, disable, or make no change to the remote MIB threshold.
	Voice	Local	Select the required option to enable, disable, or make no change to the voice (local).
		Remote	Select the required option to enable, disable, or make no change to the voice (remote).
	System	Local	Select the required option to enable, disable, or make no change to the system (local).
		Remote	Select the required option to enable, disable, or make no change to the system (remote).
	Debug	System	Select the required option to enable, disable, or make no change to the Debug (system).

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

SSH Configuration Task

You can use the SSH system-defined task to configure SSH on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Content Engine
- CSS
- NAM

For more details, see Table 4-5.

You can enter the details of this task in the SSH Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For this task to work correctly, you must use a CLI-based protocol (Telnet or SSH) as the download protocol.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Group	Sub-group	Field	Description
Common Parameters	Key Configuration	Action	Select the required option to enable, disable, or make no change to the key configuration.
IOS Parameters	Prerequisites		The Hostname and Domain name need to be configured for the devices.
	Key Configuration	Number of Key Bits [360-2048]	Enter the number of Key bits to be used for Key generation. The value must be between 360 and 2048 Key bits.
	Timeout	Action	Select the required option to add, remove, or make no change to the timeout value.
		Timeout Value [1-120):]	Enter timeout value for SSH sessions. The value should be between 1 and 120.
	Retries	Action	Select the required option to add, remove, or make no change to the number of retries.
		Number of Retries [1-5]	Enter the number of retries allowed. The number must be between 1 and 5.
CE Parameters	SSH Prerequisites	SSH Daemon	Select the required option to enable, disable, or make no change to the SSH daemon.
		Number of Key Bits [512-2048]	Enter the number of Key bits to be used for Key generation. The value must be between 512 and 2048 Key bits.
		SSH Timeout	Enter login grace time for SSH sessions, in seconds. Value must be between 1 and 99999.
		Password-guesses [1-99]	Specify the number of password retries allowed. The value must be between 1 and 99.

Group	Sub-group	Field	Description
CSS Parameters		Number of Server Key Bits [512-32768]	Enter the number of Key bits to be used for Key generation. The value must be between 512 and 32768 Key bits.
	Port	Action	Select the required option to enable, disable, or make no change to the port configuration.
		Port Number [22-65535]	Enter the port number. This value can be between 22 and 65535.
		KeepAlive	Select the required option to add, remove, or make no change to keepalive.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

TACACS Configuration Task

You can use the TACACS system-defined task to configure TACACS authentication.

This task supports the IOS device category including Cable devices.

For more details, see Table 4-5.

You can enter the details of this task in the TACACS Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Group	Sub-group	Field	Description
Common Parameters			
Server Configuration		Action	Select to enable, disable, or make no change to the TACACS Server configuration.
		Hostname or IP Address	Enter the hostname or the IP address of the TACACS server.
Login Authentication		Action	Select to enable, disable, or make no change to the login authentication details.
	Credentials	Username	Enter the username. These values are entered only in the Device and Credential Repository. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Password	Enter the enable password. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Verify	Re-enter the enable password. For details see Understanding the NetConfig Credentials Configuration Tasks.
IOS Parameters			
Server Retransmit		Action	Select to enable, disable, or make no change to the server retransmit configuration.

Group	Sub-group	Field	Description
		Retries [0-100]	Enter the number of re-tries.
Server Timeout		Action	Select to enable, disable, or make no change to the server timeout value.
		Timeout [1-1000]	Enter the timeout value.
Enable mode Authentication		Action	Select to enable, disable, or make no change to the enable mode authentication.
	Credentials	Username	Enter the username
		Password	Enter the enable password.
		Verify	Re-enter the enable password.

TACACS+ Configuration Task

You can use the TACACS+ system-defined template to configure TACACS+ on devices.

This task supports the following device categories:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- NAM

For more details, see Table 4-5.

You can enter the details of this task in the TACACS+ Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Group	Sub-group	Field	Description
Common Parameters			
TACACS Server Configuration	Server	Action	Select to enable, disable, or make no change to the TACACS Server configuration.
		Hostname or IP Address	Enter the hostname or the IP address of the TACACS server.
	Key	Action	Select to add, remove, or make no change to the TACACS encryption Key.
		Key	Enter the TACACS encryption key. The key is used to set authentication and encryption. This key must match the key used on the TACACS+ daemon. The key can be of any size.
		Verify Key	Re-enter the Key to confirm.

Group	Sub-group	Field	Description
Login Authentication		Action	Select to enable, disable, or make no change to the TACACS+ authentication. • If login authentication is enabled, then when you try to login to the device, you are authenticated by the TACACS server. • If login authentication is disabled, then you are not authenticated by the TACACS server when you log in to the device.
	Credentials	Username	Enter TACACS+ username. These values are entered only in the Device and Credential Repository. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Password	Enter TACACS+ password. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Verify	Re-enter the password to confirm. For details see Understanding the NetConfig Credentials Configuration Tasks.
IOS Parameters			
Enable mode Authentication		Action	Select to enable, disable, or make no change to the enable mode authentication.
	Credentials	Password	Enter the enable password.
		Verify	Re-enter the enable password.
	List	Name	Enter default or named list.
		Set to Default	Select to set the default list.
	Type	(Drop-down list 1)	Select the required option: • No Choice • radius • tacacs+ • line • enable • local • none Similarly, select the type from the other three drop-down lists.
	New Model	Action	Select to enable, disable, or make no change to the new model state.
CatOS Parameters			
Enable mode Authentication		Action	Select to add, remove, or make no change to the enable mode authentication.
	Credentials	Password	Enter the enable password.
		Verify	Re-enter the enable password.
	Server Options	Primary	Click to designate specified server as primary TACACS server.

Group	Sub-group	Field	Description
		All	Click to clear all hosts from the list of TACACS servers, if you selected remove in Action field.
ContentEngine Parameters	Server Option	Primary	Select to specify the server as primary.
	Password Option	ASCII Password	Select for an ACSII password.
	Connection Options	Timeout	Enter the timeout value.
		Retries	Enter the number of retries.
NAM Parameters			No category-specific commands The TACACS Server Key should be DES encrypted for NAM devices.

At the time of enabling login authentication or enable mode authentication, it is mandatory for you to enter the username and password.

At the time of disabling login authentication or enable mode authentication, these fields are optional. While disabling login authentication or enable mode authentication, if username and password are not provided, then the corresponding fields in DCR are cleared and left blank. This may make the device unreachable. Therefore we recommend that you provide the username and password at the time of disabling login authentication.

Telnet Password Configuration Task

You can use the Telnet Password system-defined configuration task to change the Telnet password on devices.

This task supports the following device categories:

- IOS (including Cable devices)
- Catalyst OS
- PIX OS

For more details, see Table 4-5.

You can enter the details of this task in the Telnet Password Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

For details on the NetConfig credentials configuration tasks, see Understanding the NetConfig Credentials Configuration Tasks.

If you change the Telnet password on a Catalyst device with an RSM module using this template, the RSM Telnet password is also changed.

The fields in the Telnet Password Configuration dialog box are:

Group	Sub-group	Field	Description
IOS Parameters	Vty Lines	Action	Select an option to enable, disable, or make no change to the Vty Line password.
		Password	Enter the Vty Line password. If you select vty, the change affects all device vty lines, and the Device and Credential Repository is updated with the new password.
		Verify	Re-enter the Vty Line password to confirm.
	Console Line	Action	Select an option to enable, disable, or make no change to the Console Line password.
		Password	Enter the Console Line password.
		Verify	Re-enter the Console Line password to confirm.
	Aux Line	Action	Select an option to enable, disable, or make no change to the Auxiliary (AUX) Line password.
		Password	Enter the Aux Line password.
		Verify	Re-enter the Aux Line password to confirm.
CatOS Parameters	Telnet Password	Action	Select an option to enable, disable, or make no change to the Telnet password. The Device and Credential Repository is updated with the new password.
		Password	Enter the Telnet password.
		Verify	Re-enter the Telnet password to confirm.
		Apply command on modules Disable will set an empty password	Select this option to update only the non IP addressable modules. If you select the Action as Disable, the password will be removed.
PIX Parameters		Action	Select the required option to replace, reset, or make no change to the password.
		Password	Enter the password.
		Verify	Re-enter the password to confirm.
		Encrypted Password	Select this option, if the password you are entering is already encrypted.

Transform System-Defined Task

You can use the Transform system-defined task to configure IPSec on devices. You must configure the IKE configuration system-defined task before configuring the Transform system-defined task.

This task supports the following device categories:

- IOS (including Cable devices)
- PIX OS

For more details, see Table 4-5.

You can enter the details of this task in the Transform Set Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Transform Set Configuration dialog box are:

Group	Sub-Group	Field	Description
IOS Parameters			
Security Association Configuration	Seconds Configuration	Seconds [120-86400]	Enter the number of seconds that will be used for negotiating IPSec security association (SA).
		Remove	Select this option to remove previously specified seconds value, if any.
	Kilo Bytes Configuration	Kilo Bytes [2560-536870912]	Enter the amount of traffic in kilobytes that will be used for negotiating IPSec SA. Value must be between 2560 and 536870912.
		Remove	Select this option to remove previously specified value, if any.
	IPSec Transform Set Configuration Note: Only for IOS 12.1 and higher.	Action	Select the required option to add, remove or make no change to transform set configuration. This sub-group of fields is applicable only to IOS version 12.1 and above.
		Transform Set Name	Enter a name for the transform set.
		Auth Header	Select the type of authentication algorithm.
		ESP Encryption	Select the type of encryption algorithm with ESP.
		ESP Authentication	Choose the type of authentication algorithm with ESP.
		IP Compression	Select to use IP compression with LZS algorithm.
		Transport Mode	Select the mode of transport.
PIX Parameters			
Security Association Configuration		Seconds [120-86400]	Enter the number of seconds that will be used for negotiating IPSec SA. The value must be between 120 and 86400 seconds.
		Kilo Bytes	Enter the amount of traffic in kilobytes that will be used for negotiating IPSec SA. The value must be between 2560 and 536870912 kilo bytes.
IPSec Transform Set Configuration		Action	Select the required option to add, remove or make no change to transform set configuration.
		Transform Set Name	Enter the name for the transform set.
		Auth Header	Select the type of authentication algorithm.

Group	Sub-Group	Field	Description
		ESP Encryption	Select the type of encryption algorithm with ESP.
		ESP Authentication	Select the type of authentication algorithm with ESP.
		IP Compression	Select to use IP compression with LZS algorithm.
		Transport	Select the mode of transport.

Web User Task

You can use the Web User configuration task to configure the web user for NAM devices. This is a System-defined task. For more details, see Table 4-5. You can enter the details of this task in the Web User Configuration dialog box.

To invoke this dialog box, see Starting a New NetConfig Job.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).. The fields in the in the Web User Configuration dialog box are:

Group	Sub-group	Field	Description
NAM Parameters	Web User	Action	Select an option to add, remove, or make no change to the web user group of fields.
		Username	Enter the username of the web user.
		Password	Enter the password for the username.
		Verify	Re-enter the password to confirm.
	Privileges	Account Management	Select the required option to enable, disable or make no change to account management.
		System Config	Select the required option to enable, disable or make no change to system configuration.
		Capture	Select the required option to enable, disable or make no change to the capture configuration.
		Alarm Config	Select the required option to enable, disable or make no change to the alarm configuration.
		Collection Config	Select the required option to enable, disable or make no change to the collection configuration.

Click **Applicable Devices** to view the devices in your selection to which this task applies.

User-defined Protocol Task

You can use the User-defined Protocol task to configure the user-defined protocol on NAM devices. This is a system-defined task.

For more details, see Table 4-5.

You can enter the details of this task in the User-defined Protocol Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the in the User-defined Protocol Configuration dialog box are:

Group	Sub-group	Field	Description
NAM Parameters	User Defined Protocol	Action	Select an option to add, remove or replace the user-defined protocol.
		Protocol	Select the protocol: • TCP • UDP
		Port [0 - 65535]	Enter the port number. You can enter any port number in the range of 0—65535.
		Name	Enter the name of the user-defined protocol.
	Affected Stats	Host	Select this option to enable host—Examines a stream of packets; produces a table of all network addresses observed in those packets (also known as the collection data). Each entry records the total number of packets and bytes sent and received by that host and the number of non-unicast packets sent by that host.
		Conversations	Select this option to enable host conversations.
		ART	Select this option to enable Application Response Time.

Click **Applicable Devices** to view the devices in your selection to which this task applies.

Cable BPI/BPI+ Task

You can use the Cable BPI/BPI+ Task to assign BPI/BPI+ options.

This task is applicable to the Cable device category. For more details, see Table 4-5.

You can enter the details of this task in the Cable BPI/BPI+ Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Cable BPI/BPI+ Configuration dialog box are:

Group	Sub-Group	Field	Description
BPI/BPI+	Interface Configuration	Cable Interface	Allows you to select an interface to modify the other fields. You must select at least one interface. Select the cable interface that you want to change.
		BPI	Select the appropriate option: • No Change—Does not change the existing configuration. • Enable—Enables this option. • Disable—Disables this option.
	Key Lifetime	Action	Select the appropriate option: • No Change—Does not modify this option. • Replace—Modifies this option to your specification. • Default—Resets this option to the system default.
		KEK Lifetime [300 - 604800]	Replaces the time (in seconds) using the specified values or resets the time using the system default. Enter time in seconds to reset the time. Enter a value from 300—604800 seconds. The default is 604800 seconds. Select the check box to reset the field to system default.
		TEK Lifetime [180 - 604800]	Replaces the time (in seconds) using your values or resets the time using the system default. Enter time in seconds to reset the time using your values. The range is 180 - 604,800 seconds and the default is 43,200 seconds. Select the check box to reset the field to system default.
	BPI/BPI+ Options	Action	Select the required options: • No Change—Does not change the existing configuration. • Enable—Enables this option. • Disable—Disables this option.
		Mandatory	Select to force all modems to use BPI.
		Authenticate Modem	Select to turn the BPI modem authentication on or off.
		Authorize Multicast	Select to turn BPI Multicast option on or off.
		OAEP Support	Select to enable or disable Optimal Asymmetric Encryption Padding (OAEP) BPI+ encryption.
		DSX Support	Select to enable or disable encryption for dynamic services SIDs.
		40 Bit Des	Select to indicate that you have chosen the 40 bit DES encryption. The system default is 56 DES encryption. This is the Cisco recommended encryption.

Click **Applicable Devices** to see the devices in your selection, to which this task applies.

Cable DHCP-GiAddr and Helper Task

You can use this task to configure the GiAddr field of DHCPDISCOVER and DHCPREQUEST packets with a relay IP address before they are forwarded to the DHCP server. You can apply this task only for a single Cable-CMTS device at a time.

This task is applicable to the Cable device category. For more details, see Table 4-5.

You can enter the details of this task in the Cable DHCP-GiAddr and Helper Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Note You can apply this task only to a single device at a time because cable templates configure interfaces on devices.

The fields in the Cable DHCP-GiAddr and Helper Configuration dialog box are:

Group	Sub-Group	Field	Description
Config Setup		Cable Interface	Select a cable interface to make the configuration changes to the selected interface, from the drop-down list. If there are no interfaces available, you will see the option No Interfaces Found in the drop-down list. You should make sure that the device is reachable and then select a valid interface.
		Action	Select an option from the drop-down list. The options are: • No Change—Does not change the current configuration. • Add/Modify—Adds a new GiAddr or Helper Address or both, or modifies an existing GiAddr or Helper Address or both.· • Remove—Removes the GiAddr or Helper Address or both.
			Select an option to Add or Modify, from the drop-down list: • DHCP-Giaddr & Helper-Address—Enables you to set the DHCP GiAddr to Policy or Primary. You can also specify values for the fields in the Cable Helper Addresses group. • DHCP-Giaddr—Enables you to set the DHCP GiAddr to Policy or Primary. • Helper-Address—Enables you to specify values for the fields in the Cable Helper Addresses group.

Group	Sub-Group	Field	Description
	Cable DHCP Giaddr	Policy Primary	Allows you to set the DHCP GiAddr to Policy or Primary: • Policy—Selects the control policy, so the primary address is used for cable modems and secondary addresses are used for hosts. • Primary—Always selects the primary address for GiAddr field. Enable this field by selecting Helper Address.
	Cable Helper Addresses	Helper Address	Allows you to enter the Helper Address to Cable Modem, Host or Host & Cable Modem.
		• Cable-Modem • Host • Host & Cable-Modem	• Cable-Modem—Specifies that only Cable Modem UDP broadcasts are forwarded. • Host—Specifies that only host UDP broadcasts are forwarded. • Host & Cable Modem—Specifies that both host and cable modem broadcasts are forwarded. Enable this field by selecting Action as DHCP GiAddr & Helper Address or by selecting Action as Helper Address.

Click **Applicable Devices** to view the devices in your selection to which this task applies.

Cable Downstream Task

You can use this task to configure the Annex, Channel-ID, Frequency, Modulation, Interleave depth, and Set rate limit of a downstream cable interface. You can also configure the Radio Frequency (RF) output of a downstream cable interface on a Cisco uBR7100 router.

This task is applicable only to Cable devices.

For more details, see Table 4-5.

You can enter the details of this task in the Downstream Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Note You can apply this task to a maximum of one Cable-CMTS device at a time.

The fields in the Downstream Configuration dialog box are:

Group	Sub-Group	Field	Description
Cable Parameters		Cable Interface	Select the required option from the drop-down list. Select a cable interface to make the required configuration changes. If you do not want to select any cable interface, choose the Not Selected option.
Activate/ Configure	Shutdown	Action	Allows you to shutdown or activate the selected interface. The options are: • No Change—Does not allow modification of any fields in this sub-group of fields. • Shutdown—Deactivates the DS port. • No Shutdown—Activates the DS port.
	Interleave Depth	Interleave Depth	Allows you to select the interleave depth of a channel. The depth can be between 8 and 128. The default is 32. Specify the interleave depth by selecting the appropriate option from the drop-down list.
		Remove	Select to remove the interleave depth configuration.
	Framing Format	MPEG Framing Format	Select the MPEG framing format from the drop-down list. The options are: • No Change—Does not allow modification of any fields in this sub-group of fields. • Annex A—For Cisco uBR-MC16E cable interface card and Cisco uBR7111E and Cisco uBR7114E Universal Broadband Routers. • Annex B—For all other Cisco cable interface cards.
		Remove	Select to remove a previously-specified MPEG framing format configuration.
	Modulation	Modulation	Sets the modulation for a downstream port on a cable interface. Select the required option. The options are: • No Change—Does not allow modification of any fields in this sub-group of fields. • 64 qam • 256 qam
		Remove	Select to remove a previously-specified modulation configuration.
	Channel	Channel ID (0-255):	Channel-ID can be from 0 and 255. Specify the channel-ID.
		Remove	Select to remove the Channel ID.
	Frequency	Frequency (54-858 MHz)	Frequency range can be from 54MHz -1,000MHz. Enter the frequency.
		Remove	Select to remove a previously-specified frequency range.

Group	Sub-Group	Field	Description
Traffic Shaping		Rate Limit	Select the required option from the drop-down list. The options are: • No Change—Does not allow modification of any fields in this group of fields. • Enable—Enables this option. • Disable—Disables this option.
		Rate Limit Algorithm (Optional):	• None—Does not modify the rest of the fields. • Token-bucket with DS Traffic Shaping—Modifies the Token Bucket Algorithm option. • Token-bucket without DS Traffic Shaping—Modifies the Token Bucket without DS Traffic Shaping Algorithm option • Weighted-discard—Modifies the Weighted Discard option.
	Token Bucket (Optional)	Granularity in Milli seconds (Optional):	Specifies traffic shaping granularity in milliseconds. This field is enabled only if you have selected the Rate Limit Algorithm as Token-bucket with DS Traffice Shaping. Select the required value from the drop-down list. You can choose a value between 1 and 16 msec.
		Max Delay in Milli seconds (Optional):	Sets the maximum buffering delay in milliseconds. This field is enabled only if you have selected the Rate Limit Algorithm as Token-bucket with DS Traffice Shaping. Select the required value from the drop-down list. You can choose a value between 128 and 1024.
	Weighted Discard (1-4) (Optional)	Weight for the exponential moving average of loss rate	Sets the weighted discard algorithm. This field is enabled only if you have selected the Rate Limit Algorithm as Weighted Discard. Enter a weight between 1 and 4.

Click **Available Devices** to view the list of devices from your selection, to which this task applies.

Cable Upstream Task

Use this task to configure the frequency, minislot size, power level and admission control on upstream cable interfaces. You can apply this task to a maximum of one Cable-CMTS device at a time.

This task is applicable only to Cable devices.

For more details, see Table 4-5.

You can enter the details of this task in the Upstream Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Note You can apply this task to a maximum of one cable device at a time.

The fields in the Upstream Configuration dialog box are:

Group	Sub-Group	Field	Description
Config Setup		Cable Interface	Allows you to select cable interfaces for configuration. Select the cable interfaces from the drop-down list.
	Activate/ Deactivate US Port	Activate/Deactivate	Select one of these options from the drop-down list. The options are: • No Change—Does not change the existing configuration. • Shutdown—Deactivates this port. • No Shutdown—Activates this port.
Frequency		Value [5-42 MHz]	Enter the required frequency value in the range 5—42 MHz. The range for the frequency is: • 5—65 MHz for Cisco uBR-MC16E cable interface line card • 5—42 MHz for all other cable interface line cards.
		Set to Default	Select this option to set the default frequency. A negation command is generated to remove the frequency value and set the default. This is because the default frequency value is dynamic and varies from device to device.
Power Configuration	Power Level	Value [-10-+25 dBmV]:	Enter the power level. The valid range for the power level is between -10dBmV and +25dBmV.
		Set to Default	Select this option to set the default power level. The default is 0dBmV.
	Power Adjustment	Continue [2-15 dB]	Enter the power adjustment value. The valid range for power adjustment value is between 2dB and 15dB.
		Set to Default	Select this option to set the default power adjustment value. The default is 2dB.
		Noise	Enter the power adjustment noise level. The valid range for the power adjustment noise value between 10 and 100%.
		Set to Default	Select this option to set the default noise value. The default is 30%.
		Threshold [0-10 dB]	Enter the power adjustment threshold value. The valid range for the power adjustment threshold value is between 1dB and 10dB.
		Set to Default	Select this option to set the default power adjustment threshold value. The default is 1dB.

Group	Sub-Group	Field	Description
Admission Control		Value [0 - 1000%]	Indicates the maximum cumulative bandwidth reservation allowed before new CMs are rejected. The valid range is between 10% and 1000%.
		Set to Default	Select this option to set the default admission control value. The default value is 100%.
Minislot Size		Size	Select the required options. The options are: • No Change • 2 • 4 • 8 • 16 • 32 • 64 • 128 • [default] Select **No Change** to make no changes in this field.
Channel Width(Hz)		Size	Select the required channel width option. The options are: • No Change—Does not modify the existing configuration. • 200000 • 400000 • 800000 • 1600000 (default) • 3200000 Select **No Change** to make no changes in this field.
Concatenation		Concatenation	Select one of these options: • No Change—Does not modify the existing configuration • Enable—Enables this option. • Disable—Disables this option.
FEC		FEC	Select one of the following options for Enable Forward Error Correction (FEC): • No Change - Does not modify the existing configuration. • Enable - Enables this option. • Disable - Disables this option.
Fragmentation		Fragmentation	Select the required fragmentation option. The options are: • No Change—Does not modify the existing configuration. • Enable—Enables this option. • Disable—Disables this option.

Group	Sub-Group	Field	Description
Rate Limit		Rate Limit	Select the required rate limit option. The options are: • No Change—Does not modify the existing configuration. • Enable—Enables this option. • Disable—Disables this option.
		Apply Token Bucket Algorithm	Click the check box to apply this option.
		Enable Traffic Shaping	Click the check box to apply this option.
Data Backoff		Data Backoff	Select the required data backoff option. The options are: • No Change—Does not modify the existing configuration. • Enable—Enables this option. • Disable—Disables this option. If you choose **Enable**, you can perform data back off automatically, or manually by entering the start and end values.
		Automatic	Choose this to apply a default value for data automatically.
		Start Value [0-15]	Enter the start value. The valid range for the start value is 0 and 15. There is no default value.
		End Value [0-15]	Enter the end value. The valid range for the end value is 0 and 15. There is no default value.
Range Backoff		Range Backoff	Select one of these options: • No Change—Does not modify the existing configuration. • Enable—Allows you to perform data back off automatically, or manually by entering the start and end values. • Disable—Disables this option.
		Automatic	Select this, to apply a range back-off value automatically.
		Start Value (0-15)	Enter the start value. The valid range for the start value is 0-15. There is no default value.
		End Value (0-15)	Enter the end value. The valid range for the end value is 0-15. There is no default value.

Click **Available Devices** to view the list of devices from your selection, to which this task applies

Cable Interface Bundling Task

You can use this task to configure the interface bundling. You can apply this task only to a single Cable-CMTS device at a time.

This task is applicable to the Cable device category. For more details, see Table 4-5.

You can enter the details of this task in husbanded Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Note At a time, you can apply this task only to a single device, because cable templates configure interfaces on devices.

The fields in the Bundle Configuration dialog box are:

Group	Field	Description
Cable Parameters	Action	Select one of these options: • No Change—Does not modify the existing parameters. • Add—Enables you to configure an interface as a master interface or a slave interface. • Remove—Enables you to change the previous configuration of the interface (master to slave or vice versa). Choose the option from the drop down list.
	Bundle ID (1-255)	Indicates the bundle identifier. Enter a bundle ID between 1 and 255.
	Master Interface	Allows you to configure the primary interfaces. Select the cable interface from the list of primary interfaces. Select **Not Selected** if you do not want to select a primary interface.
	Slave Interface	Allows you to configure the secondary interfaces. Select the cable interface from the list of secondary interfaces. Select **Not Selected** if you do not want to select a secondary interface.

Click **Applicable Devices** to view the devices in your selection to which this task applies.

Cable Spectrum Management Task

You can use this task to create and assign spectrum groups to cable interfaces and upstream interfaces.

This task supports cable devices.

For more details, see Table 4-5.

You can enter the details of this task in the Cable Spectrum Management Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Cable Spectrum Management Configuration dialog box are:

Group	Sub-Group	Field	Description
Spectrum Management	Spectrum Group	Action	Select one of these options: • No Change—Does not allow you to make any changes in the Spectrum group of fields. • Add—Allows you to add options. • Remove—Allows you to remove options.
		Spectrum Group ID [1 - 32]	Enter the Spectrum Group ID. The range for Spectrum Group ID is 1—32.
		Frequency Setting	Select one of these frequency settings: • Band—Enter a range of frequencies. • Fix—Enter a fixed frequency.
		Start Frequency [5 - 42 MHz]	Enter the start frequency. The range of frequencies is: • uBR-MC16E cable interface card • 5MHz—65MHz for Cisco • 5MHz—42MHz for all other cable interface cards
		End Frequency [5 - 42 MHz]	Enter the end frequency. The range of frequencies is: • uBR-MC16E cable interface card • 5MHz—65MHz for Cisco • 5MHz—42MHz for all other cable interface cards. This field is enabled only if you choose **Fix** as the value in the Frequency Setting filed, in the Spectrum Group.
	Optional Configuration	Power Level [-10 - 25 dBmV]	Enter the Power Level. The valid power levels are between -10dBmV and +25dBmV. The default is 0dBmV.
		Hop Period [5 - 300 Sec]	Enter the Hop period. The valid range for a Hop Period (in seconds) is between 1 and 3600. The default for Advanced Spectrum Management is 25 seconds. For all others, the default is 300 seconds. This field is enabled only if you choose **Add** as the value in the Action field, in the Spectrum Group.
		Hop Threshold [0 - 100%]	Enter the Hop Threshold. The valid range for Hop Threshold is between 1 and 100%. The default is 20%. This field is enabled only if you select **Add** as the value in the Action field, in the Spectrum Group.

Group	Sub-Group	Field	Description
		Shared RF Spectrum Group Configuration	Indicates that the upstream ports in a spectrum group can share the same upstream frequency.
	Schedule	Schedule	Select one of these options from the drop down list: • No Change—Does not allow you to enter the scheduling information. • Add—Allows you to add a scheduled task. • Delete—Allows you to delete a scheduled task.
		Schedule Day	Select the schedule day from the drop-down list.
		Schedule Time (hh:mm:ss)	Enter the schedule time in the hh:mm:ss format.
	Interface Assignment	Action	Select one of these option from the drop-down list: • No Change—Does not allow changes to the existing assignment. • Assign—Allows you to assign an interface. • Unassign—Allows you to unassign an interface.
		Cable Interface	Select a cable interface from the drop-down list.
		Spectrum ID [1 - 32]:	Enter the Spectrum ID. The range for Spectrum ID is between 1 and 32. This field is disabled if you chose **Unassign** as the value in the Action field, in the Interface Assignment sub-group.

Click **Applicable Devices** to view the devices in your selection to which this task applies.

Cable Trap Source Task

You can use this task to configure SNMP Traps hosts, notification, message and notification of SNMP Traps on a cable interface.

This task supports cable devices.

For more details, see Table 4-5.

You can enter the details of this task in the Trap Source Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Trap Source Configuration dialog box are:

Group	Sub-Group	Field	Description
Trap Source Configuration	Trap Source Interface	Action	Select the required option to add, remove or make no change to a Trap Source interface.
		Trap Source Interface	Select the required trap source interface from the drop-down list.

Group	Sub-Group	Field	Description
	CM On/Off Trap Interval	Cable Interface	Select the cable interface on which to specify the trap interval.
		Interval [0 - 86400]	Specify a value for the trap interval in the range 0 and 86400 seconds.
		Set to Default	Select this to set the trap interval to the default value of 600 seconds.

Click **Applicable Devices** to view the devices in your selection to which this task applies.

Support for Auto Smartports and Smartports

Smartport macros provide an easy way to save and share common configurations. Each Smartport macro is a group of CLI commands. When you apply a Smartport macro on a port, the CLI commands within the macro will be deployed on the port. If the command fails when applying a macro, either due to a syntax error or a configuration error, the macro continues to apply the remaining commands on the port.

Auto Smartports macros apply the configuration commands on a port automatically based on the policy definitions configured in the device.

As part of provisioning Smartports and Auto Smartports, LMS provides the following Netconfig tasks:

- Auto Smartports—Task applicable for Device based Netconfig flow
- Manage Auto Smartports—Task applicable for Port based Netconfig flow
- Smartports—Task applicable for Port based Netconfig flow

Auto Smartports

LMS allows you to configure Auto Smartports macro policies on a device.

If Auto Smartports macro is enabled at device level, all the available ports in the device will be enabled for auto smartports, except for the ports that are in disabled state.

You can use the Auto Smartports task to:

- Enable or disable auto smartports functionality at device level
- Apply or remove auto smartports policy definitions

You can enter the details of this task in the Auto Smartports Configuration dialog box.

To invoke this dialog box, see Starting a New NetConfig Job.

Note The Auto Smartports task is available only in the Device based flow of a NetConfig job. For applying Auto Smartports task, the minimum supported version of the IOS image should be 12.2(50) SE.

The fields in the Auto Smartports Configuration dialog box are:

Group	Field	Description
IOS Parameters		
Enable/Disable Auto Smartports	Action	You can select the following actions to enable or disable auto smartports functionality at device level: • Enable—Select this action to enable auto smartports • Disable—Select this action to disable auto smartports
	Enable CDP fallback	Check to enable CDP fallback.
Built-in Auto Smartports macro	Event trigger identifier	Select the following event trigger identifier from the drop-down list: • CISCO_PHONE_EVENT • CISCO_ROUTER_EVENT • CISCO_SWITCH_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
	Associated macro	The macro associated with the event trigger identifier. The field is automatically populated based on the event trigger identifier selected. The following are the macros associated with the event trigger identifier: • CISCO_PHONE_AUTO_SMARTPORT—Macro associated with the event trigger identifier CISCO_PHONE_EVENT • CISCO_SWITCH_AUTO_SMARTPORT—Macro associated with the event trigger identifier CISCO_SWITCH_EVENT • CISCO_ROUTER_AUTO_SMARTPORT—Macro associated with the event trigger identifier CISCO_ROUTER_EVENT • CISCO_AP_AUTO_SMARTPORT—Macro associated with the event trigger identifier CISCO_WIRELESS_AP_EVENT • CISCO_LWAP_AUTO_SMARTPORT—Macro associated with the event trigger identifier CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
	Access VLAN	Enter the Access VLAN value. The value entered must be greater than zero. For example, 2. By default, the value for Access VLAN will be 1. This field is enabled only if you have selected the following event trigger identifier: • CISCO_PHONE_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT

Group	Field	Description
	Voice VLAN	Enter the Voice VLAN value. The value entered must be greater than zero. For example, 1. By default, the value for Voice VLAN will be 2. This field is enabled only if you have selected the event trigger identifier CISCO_PHONE_EVENT
	Native VLAN	Enter the Native VLAN value. The value entered must be greater than zero. For example, 1. By default, the value for Native VLAN will be 1. This field is enabled only if you have selected the following event trigger identifier: • CISCO_ROUTER_EVENT • CISCO_SWITCH_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
User-defined Auto Smartports macro	Action	You can select the following actions to apply or remove auto smartports policy: • Apply—Select this action to define auto smartports policy • Remove—Select this action to remove the existing auto smartports policy
	Event trigger type	Select the following event trigger type: • Pre-defined trigger—To associate the auto smartports macro with a pre-defined event trigger. • User-defined trigger—To associate the auto smartports macro with a user-defined event trigger.
	Event trigger identifier	Select the following event trigger identifier from the drop-down list: • CISCO_PHONE_EVENT • CISCO_ROUTER_EVENT • CISCO_SWITCH_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT This drop-down list is enabled only if you have selected the Event trigger type as Pre-defined trigger.
	User-defined event trigger identifier	Enter the name of the event trigger identifier. This field is enabled only if you have selected the Event trigger type as User-defined trigger.

Group	Field	Description
	User defined macro input mode	Enter the auto smartports CLI commands either through CLI command interface or import from a file (.txt) that has CLI commands. You can select the following options: • CLI command • Import CLI command from the file

	Macro command(s)	Enter the CLI commands.
		For example,
		`if [[ $LINKUP -eq YES ]]; then`
		`conf t`
		`interface $INTERFACE`
		`macro description $TRIGGER`
		`switchport access vlan 1`
		`exit`
		`end`
		`fi`
		`if [[ $LINKUP -eq NO ]]; then`
		`conf t`
		`interface $INTERFACE`
		`no macro description`
		`no switchport access vlan 1`
		`exit`
		`end`
		`fi`
		This field is enabled only if you have selected the User-defined macro input mode as CLI command.

Select macro command input file from the server	Files	Click **Browse** and select the file (.txt) that has the CLI commands. The CLI command file (.txt) should reside in the default location: • On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/netconfig/ • On Windows: *NMSROOT*\files\rme\netconfig\ Where, *NMSROOT* is the LMS install directory.
Applicable Devices (Button)		Allows you to view the IOS devices in your selection on which you want to configure Auto Smartports macros.
Save (Button)		Saves the information you have specified.
Reset (Button)		Clears all fields and reverts to the default setting.
Cancel (Button)		Ignores your changes.

Manage Auto Smartports

You can use the Manage Auto Smartports task to enable or disable auto smartports functionality on a port.

You can enter the details of this task in the Manage Auto Smartports Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note The Manage Auto Smartports task is available only in the Port based flow of a NetConfig job.

The fields in the Manage Auto Smartports Configuration dialog box are:

Group	Field	Description
IOS Parameters		
	Action	Select the following actions: • **Enable**—Enables auto smartports functionality on the port. • **Disable**—Disables auto smartports functionality on the port.
	Enable Auto Smartports at device level	Check the checkbox to enable auto smartports at a device level.
	Enable CDP fallback	Check to enable CDP fallback.
Applicable Devices (Button)		Allows you to view the IOS devices in your selection on which you want to configure auto smartports macros.
Save (Button)		Saves the information you have specified.
Reset (Button)		Clears all fields and reverts to the default setting.
Cancel (Button)		Ignores your changes.

When you schedule a NetConfig job for Manage Auto Smartports task and if you have selected any of the following Failure Policies, in the Job Schedule and Options dialog box, the rollback functionality will happen only if the archived configuration contains the command `macro auto global processing [cdp-fallback]`.

- Rollback device and stop
- Rollback device and continue
- Rollback job on failure

Smartports

You can use the Smartports task to apply Smartports to a port by selecting the predefined smartports macros.

You can enter the details of this task in the Smartports Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note The Smartports task is available only in the Port based flow of a NetConfig job.

The fields in the Smartports Configuration dialog box are:

Group	Field	Description
IOS Parameters		
Built-in Smartport Macro	Smartport Macro	Select the following predefined smartport macros from the drop-down list: • cisco-desktop • cisco-phone • cisco-switch • cisco-router • cisco-wireless
	Access VLAN	Enter the Access VLAN value. The value entered must be greater than zero. For example, 2. This field is enabled only if you have selected the following smartports macros: • cisco-desktop • cisco-phone
	Voice VLAN	Enter the Voice VLAN value. The value entered must be greater than zero. For example, 1. This field is enabled only if you have selected cisco-phone as the smartports macro.
	Native VLAN	Enter the Native VLAN value. The value entered must be greater than zero. For example, 1. This field is enabled only if you have selected the following smartports macro: • cisco-switch • cisco-router • cisco-wireless
Applicable Devices (Button)		Allows you to view the IOS devices in your selection on which you want to configure auto smartports macros.
Save (Button)		Saves the information you have specified.
Reset (Button)		Clears all fields and reverts to the default setting.
Cancel (Button)		Ignores your changes.

When you schedule a NetConfig job for Smartports task and if you have selected any of the following Failure Policies, in the Job Schedule and Options dialog box, the rollback functionality will not happen.

- Rollback device and stop
- Rollback device and continue
- Rollback job on failure

PoE Task

You can use the PoE task to configure Power and Power Policing in ports. Power Policing allows you to turn off power while generating syslogs. This is needed if the real-time power consumption exceeds the maximum power allocation on the port.

Power policing and ePoE are supported only on Catalyst 3750-E and Catalyst 3560-E switches with PoE ports.

You can enter the details of this task in the PoE Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note The PoE task is available only in the Port based flow of a NetConfig job.

The fields in the PoE Configuration dialog box are:

Field	Description
Power Management	
Power Mode	Select the following power modes: • Auto • Static • Disable If you select Disable as the power mode, the detection and power for the inline power capable interface will be disabled.
Max Power	Enter the maximum power for the selected mode. Maximum power can be upto 20,000 milliwatts.
Power Policing	
Policing	Select the following options for power policing: • Enable • Disable
On Violation	Select the following to either generate a Syslog or to turn off power to the device. • Generate Syslog • Turn-Off Power
Applicable Devices	Allows you to view the IOS devices in your selection on which you want to configure PoE policies.

Field	Description
Save (Button)	Saves the information you have specified.
Reset (Button)	Clears all fields and reverts to the default setting.
Cancel (Button)	Ignores your changes.

You can generate PoE MAX Power Violation syslog report for this task. See *Reports Management with Cisco Prime LAN Management Solution 4.1* for more information.

Catalyst Integrated Security Features

You can use the Catalyst Integrated Security Features task to configure Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard and Security Violation on ports.

The Catalyst Integrated Security Feature is supported only on Catalyst 2960, 3560, 3560E, 3750, 3750E switches.

You can enter the details of this task in the Catalyst Integrated Security Features Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note The Catalyst Integrated Security Features task is available only in the Port based flow of a NetConfig job.

The fields in the Catalyst Integrated Security Features Configuration dialog box are:

Field	Description
IOS Parameters	
Port Security	
Action	Select the following actions to limit the number of MAC addresses that can be learned through a port: • Change • Disable
Maximum Number of MAC Addresses	Enter the number of MAC addresses. This field is enabled only if the action Change is selected.

Field	Description
Security Violation	Select the following security violation modes for a port: • Protect—Packets with unknown source addresses are dropped until the sufficient number of secure MAC addresses drops below the maximum value. • Restrict—Packets with unknown source addresses are dropped until the sufficient number of secure MAC addresses drops below the maximum value, and the Security Violation counter is incremented. • Shutdown—Interface immediately goes into an error-disabled state and sends an SNMP trap notification. • Disable—Disables security violations
DHCP Snooping	
Global DHCP Snooping	Enables or disables DHCP Snooping globally.
VLAN DHCP Snooping	Enables or disables DHCP Snooping only on VLAN.
VLAN ID or VLAN Range	Enter the VLAN ID or VLAN range or both. For example, • You can enter the VLAN ID as 10. • You can enter the VLAN range separated by a space or a hypen as 1 4,4-8. • You can enter both VLAN ID and VLAN range as 10, 4-8.
Port Trusting	Configure port trusting by selecting the following options: • Trust • UnTrust
DHCP Messages Per Second	Configure the DHCP messages rate limit for the ports and enter the number of DHCP messages that can be received per second.
Dynamic ARP Inspection	
VLAN Dynamic ARP Inspection	Enables or disables Dynamic ARP Inspection only on VLAN.
VLAN ID or VLAN Range	Enter the VLAN ID or VLAN range or both. For example, • You can enter the VLAN ID as 10. • You can enter the VLAN range separated by a space or a hypen as 1 4,4-8. You can enter both VLAN ID and VLAN range as 10, 4-8.
Port Trusting	Configure port trusting by selecting the following options: • Trust • UnTrust
ARP Messages Per Second	Configure the ARP messages rate limit for the ports and enter the number of ARP request messages that can be received per second.
IP Source Guard	

Field	Description
Action	Configure the IP souce guard by selecting the following actions: • Enable Filter By Source IP • Enable Filter By Source IP and MAC Address • Disable Filter By Source IP • Disable Filter By Source IP and MAC Address
Applicable Devices	Allows you to view the IOS devices in your selection on which you want to configure Catalyst Integrated Security Features on the ports.
Save (Button)	Saves the information you have specified.
Reset (Button)	Clears all fields and reverts to the default setting.
Cancel (Button)	Ignores your changes.

You can generate a Syslog Analyzer report for this task, which lists only the Syslogs that are specific to Catalyst Integrated Security Features. See *Reports Management with Cisco Prime LAN Management Solution 4.1* for more information.

EEM Environmental Variables Task

You can use this task to configure EEM Environmental Variables (that are used by the TCL script) on Cisco Catalyst 6500, 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches.

You can enter the details for this task in the Environmental Variables Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

The fields in the EEM Environmental Variables Configuration dialog box are:

Field/Button	Description
IOS Parameters	
EEM Environmental Variables	
Action	Select either: • **Add** - to add one or more variables. Or • **Remove** - to remove one or more variables.
Variable Name	Enter the name for the variable. Example: `my_counter` You can create a maximum of five variables at a time. If you want to create more variables, create another instance by clicking Add Instance Button.

Field/Button	Description
Value	Enter the value for the variable. Example: `15` Now the variable `my_counter` will have the value `15`.
Applicable Devices	Allows you to view the IOS devices in your selection, to which these variables would be applied to.
Save	Saves the information you have specified.
Reset	Clears all fields and reverts to the default setting.
Cancel	Ignores your changes.

Embedded Event Manager Task

You can use this task to configure EEM Scripts or Applets on Cisco Catalyst 6500, 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches.

You can enter the details for this task in the Embedded Event Manager Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

The fields in the Embedded Event Manager Configuration dialog box are:

Field/Button	Description
IOS Parameters	
EEM Configuration	
Policy Type	Select either **Script** or **Applet** as the policy.
Action	Select **Register** or **Unregister** to register or unregister a script or applet.

Field/Button	Description
Device Directory Options	
Create New Directory	Check this option if you want to create a new directory on the device to copy the applet or script. If you select this checkbox, the input given in the Directory Name textbox is used to create a new directory. This option is activated only when the Script Policy and Register Action options are selected.
Directory Name	Enter the absolute path of the directory where the file needs to be placed on the device. Example: `disk0:/Testing` Here a new directory Testing is created in the device under disk0 Partition. Ensure that the selected directory has enough space before the script files are copied. This option is activated only when the Script Policy and Register Action options are selected.
Upload Script/Applet files from Server	
Files	Use this option to either: • Enter the file location to upload the scripts to deploy on the device. Ensure that you enter the absolute path along with the filename. You can specify multiple filenames separated by commas. Or • Browse to the directory and select one or more scripts to deploy on the device. – Use CTRL to select more than one file. – Use **Browse** to browse to the directory. You cannot combine tcl files and applet files in a single NetConfig task.
Applicable Devices	Allows you to view the IOS devices in your selection, to which the scripts or applets apply.
Save	Saves the information you have specified.
Reset	Clears all fields and reverts to the default setting.
Cancel	Ignores your changes.

For more information, see *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1*.

EnergyWise Configuration Task

You can use the EnergyWise Configuration Task to configure EnergyWise on devices.

You can enter the details of this task in the EnergyWise dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note The EnergyWise Configuration task is available only in the Device based flow of a NetConfig job.

The fields in the EnergyWise Configuration dialog box are:

Field	Description
IOS Parameters	
Enable/Disable EnergyWise	
Configure EnergyWise	Select the following options to enable or disable EnergyWise configuration on the devices: • **Enable**—To enable EnergyWise configuration on the devices • **Disable**—To disable EnergyWise configuration on the devices • **No Change**—To make no change to the EnergyWise configuration on the device.
Domain Configuration	
EnergyWise Entity Domain	Enter an EnergyWise domain name. For example, myDomain This field is disabled if you have selected **Disable** as the Configure EnergyWise option.
EnergyWise Entity Secret	Enter the EnergyWise Entity secret name. This field is disabled if you have selected **Disable** as the Configure EnergyWise option.
Advanced Configuration	
Entity Importance (1-100)	Enter the value for EnergyWise Importance. Importance allows you to differentiate among devices in the domain. The value for Importance ranges from 1 to 100, where a value of 1 is the lowest and a value of 100 is the highest. This field is disabled if you have selected **Disable** as the Configure EnergyWise option.
Entity Keywords (comma separated)	Enter the keyword. For example, myLobbyphones. You can set Keyword to identify a specific device or group of devices. You can use these keywords to query the devices for specific data. This field is disabled if you have selected **Disable** as the Configure EnergyWise option.
Entity Role	Enter the role for a specific device or device group access. This field is disabled if you have selected **Disable** as the Configure EnergyWise option.

Field	Description
EnergyWise Level	Select the following EnergyWise level to be configured on the devices: • 0 - Shut • 1 - Hibernate • 2 - Sleep • 3 – Standby • 4 – Ready • 5 – Low • 6 – Frugal • 7 – Medium • 8 – Reduced • 9 – High • 10 - Full This drop-down list is disabled if you have selected **Disable** as the Configure EnergyWise option.
Management Configuration	
EnergyWise Port Number	Enter the EnergyWise port number that sends and receives queries. The range is from 1 to 65000. The default is 43440. After entering the EnergyWise port number, you must select either: • Interface—Select **Interface** and specify the EnergyWise Interface ID. Or • IP Address—Select **IP Address** and specify the EnergyWise IP Address. Or • Use Mgmt IP Address of Devices—Select to use the management IP Address of devices added in the DCR.
EnergyWise Interface	Specify the EnergyWise Interface ID from which the EnergyWise messages are sent. For example, FastEthernet0/2.
EnergyWise IP Address	Specify the EnergyWise IP Address from which the EnergyWise messages are sent.
Applicable Devices (Button)	Allows you to view the IOS devices in your selection on which you want to configure EnergyWise.
Save (Button)	Saves the information you have specified.
Reset (Button)	Clears all fields and reverts to the default setting.
Cancel (Button)	Ignores your changes.

For more information, see *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1*.

EnergyWise Parameters Task

You can use the EnergyWise Parameters task to configure EnergyWise on ports. You can enter the details of this task in the EnergyWise Parameters Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note The EnergyWise Parameters task is available only in the Port based flow of a NetConfig job.

The fields in the EnergyWise Parameters Configuration dialog box are:

Field	Description
Configure EnergyWise Parameters	
Entity Keywords (comma separated)	Enter the keyword name. Keywords can be set to identify a specific interface or group of interfaces. For example, lab1
Entity Role	Enter the role for a specific device or device group access. For example, lobbyaccess
Entity Importance (1-100)	Enter the value for Importance. Allows you to differentiate among devices in the domain. The value for Importance ranges from 1 to 100, where a value of 1 is the lowest and a value of 100 is the highest.
Applicable Devices (Button)	Allows you to view the IOS devices in your selection on which you want to configure EnergyWise.
Save (Button)	Saves the information that you have specified.
Reset (Button)	Clears all fields and reverts to the default setting.
Cancel (Button)	Ignores your changes.

EnergyWise Events Task

You can use the EnergyWise Events task to configure EnergyWise events on ports of EnergyWise supported devices.

You can enter the details of this task in the EnergyWise Events Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

Note The EnergyWise Events task is available only in the Port-based flow of a NetConfig job.

The fields in the EnergyWise Events Configuration dialog box are:

Field	Description
IOS Parameters	
Action	Select the following actions to enable or disable EnergyWise events on ports: • Enable—To enable EnergyWise events configurations on ports • Disable—To disable EnergyWise events configurations on ports
EnergyWise Level	Select the following EnergyWise event levels: • 0 - Shut • 1 - Hibernate • 2 - Sleep • 3 – Standby • 4 – Ready • 5 – Low • 6 – Frugal • 7 – Medium • 8 – Reduced • 9 – High • 10 - Full This drop-down list is disabled if you have selected Disable as the Action.
Recurrence	
Configure Recurrence level	Check the checkbox to configure event recurrence level.
Importance (1-100)	Enter the value for Importance. Allows you to differentiate among devices in the domain. The value for Importance ranges from 1 to 100, where a value of 1 is the lowest and a value of 100 is the highest.
Hour [00 - 23]	Select the hour interval to configure the event recurrence interval. You can select the hourly time between 00 and 23 hours.
Minute [00 - 59]	Select the minute interval to configure event recurrence interval. You can select the minute interval between 00 and 59 minutes
Month [1 - 12]	Enter the month in number format, separated by comma. You can enter the value for one month [3], or for a range of months [7-9], or both [3, 7-9]. If this field is left blank, the Netconfig job considers the value as applied for all the months [1-12].
Day of the Month [1 - 31]	Enter the day of the month in number format, separated by comma. You can enter the value for one day [20], or for range of days [15-19], or both [10, 15-20]. If this field is left blank, the Netconfig job considers the value applied for all the days of a month [1-31].

Field	Description
Day of the Week	Select the day of the week by checking the checkbox. If all the days of the week are left unchecked, the Netconfig job considers the value being checked for all the days of a week [Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday].
Time Range	Enter the EnergyWise IOS time-range configured in the Global Config mode. For example, if you have configured the time range “Periodic Friday 07:00 to 20:00” to a time-range name “Friday” in the Global Config mode in the EnergyWise IOS, you must enter “Friday” in this Time Range field. This option is applicable for EnergyWise enabled devices running EnergyWise 2.0 software image.
Applicable Devices (Button)	Allows you to view the IOS devices in your selection.
Save (Button)	Saves the information that you have specified.
Reset (Button)	Clears all fields and reverts to the default setting.
Cancel (Button)	Ignores your changes.

GOLD Boot Level Task

You can use this task to configure Boot Level Diagnositc tests on the following device category:

Cisco Catalyst 6500 devices

You can enter the details for this task in the GOLD Boot Level Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

The fields in the GOLD Bootup Level Configuration dialog box are:

Field/Button	Description
Action	Select either **Enable** to enable the actions or **Disable** to disable the actions
Level	Select either **Complete** to set the boot level to Complete or **Minimal** to set the boot level to Minimal This option is activated only if the Action option is enabled. This option is not activated, if you have selected **Disable** in the Action field.
Save	Saves the information you have specified.
Reset	Clears all fields and reverts to the default setting.
Cancel	Ignores your changes.

For more information, see *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1*.

GOLD Monitoring Test Task

You can use this task to configure GOLD Monitoring tests on the following device categories:

- Cisco Catalyst 6500 IOS switches
- Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E Switches

You can enter the details of this task in the GOLD Monitoring Tests Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

The fields in the GOLD Monitoring Test Configuration dialog box are:

Pane	Description
GOLD Monitoring Test Configuration	
Configuring Health Monitoring Diagnostics	
Action	Select any of the following: • **Add Interval** - To add an interval • **No Interval**. - To not add an interval • **No Change** - To make no change
Enter Vendor Type or Name	Enter the Vendor type or Module Name. You can enter one or more comma separated module names. Example: cevCat6kVsS72010G This is a mandatory field and is available only if you select Cisco Catalyst 6500 devices.
Enter Switch ID	Enter the Switch ID. You can enter a single switch ID or a number of switch IDs separated by comma. Example 1: Enter **2** if you want to include switch with ID 2. Example 2: Enter **3, 6** if you want to include switches with IDs 3 and 6. This is a mandatory field and is available only if you select Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, or 3750E stack switches.
Enable/Disable Health Monitoring Diagnostics Test	
Action	Select any of the following: • **Enable** - To start the Health Monitoring tests • **Disable** - To stop the running Health Monitoring tests. The tests once stopped, will not start again until the Action is enabled. • **No Change** - No change to Action
Test Details	
All	Allows you to configure all diagnostic tests.
Enter Testnames	Allows you to manually enter the test names. Enter one or more test names separated by comma. This option is activated only if the Enable Action is selected.

Pane	Description
Range	Allows you to enter a range for tests to be run. This option is activated only if the Enable Action is selected. Example: Enter **2-8** if you want to run tests with IDs from 2 to 8.
Configure Health Monitoring Interval	
No. of Days	Enter the number of days till which you require the tests to be run on the devices. The number of days can be any value between 0 - 20. The default value is 1 day.
Hours	Select the hour frequency at which the tests should be run. You can enter any value between 00 and 23 for hour. This is a mandatory field and is enabled only if you have selected **Add Interval**.
Minutes	Select the minute frequency at which the tests should be run. You can enter any value between 00 and 59 for the minute. This is a mandatory field and is enabled only if you have selected **Add Interval**.
Seconds	Enter the seconds frequency at which the tests should be run. You can enter any value between 00 and 59 for the second. This is a mandatory field and is enabled only if you have selected **Add Interval**.
Milliseconds	Enter the millisecond frequency at which the tests should be run. You can enter any value between 0 and 999 for the second. This is a mandatory field and is enabled only if you have selected **Add Interval**.
Applicable Devices	Allows you to view the IOS devices in your selection that you want to monitor with GOLD Monitoring Tests.
Save	Saves the information you have specified.
Reset	Clears all fields and reverts to the default setting.
Cancel	Ignores your changes.

For more information, see *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1*.

GOLD Health Monitoring Test Task

You can use this task to configure GOLD Health Monitoring tests on Cisco Catalyst 6500 IOS switches device categories.

This task is available only for the Module-based netconfig job wizard.

You can enter the details of this task in the Gold Health Monitoring Test Configuration dialog box. To invoke this dialog box, see Create a NetConfig Job based on Module or Port.

The fields in the GOLD Health Monitoring Test Configuration dialog box are:

Pane	Description
GOLD Health Monitoring Test Configuration	
Configuring Health-Monitoring Diagnostics for Cat6k Devices	
Action	Select any of the following: • **Run Test** - To run a test • **Add Test** - To add a test • **Remove Test** - To remove a test
Test Details	
All	Allows you to configure all diagnostic tests.
Pre-defined	Allows you to select the following pre-defined tests: • TestLoopback • TestNetflowInlineRewrite • TestEobcStressPing • TestFirmwareDiagStatus • TestAsicSync
Enter Testnames	Allows you to manually enter the test names. Enter one or more test names separated by comma.
Range	Allows you to enter a range for tests to be run. Example: Enter **2-8** if you want to run tests with IDs from 2 to 8.
Configure Health Monitoring Interval	
No. of Days	Enter the number of days till which you require the tests to be run on the devices. The number of days can be any value between 0 - 20. The default value is one day. This field is enabled only if you have selected **Add Test**.
Hours	Select the hour frequency at which the tests should be run. You can enter any value between 00 and 23 for the hour. This field is enabled only if you have selected **Add Test**.
Minutes	Select the minute frequency at which the tests should be run. You can enter any value between between 00 and 59 for the minute. This field is enabled only if you have selected **Add Test**.
Seconds	Enter the seconds frequency at which the tests should be run. You can enter any value between 00 and 59 for the second. This field is enabled only if you have selected **Add Test**.
Milliseconds	Enter the millisecond frequency at which the tests should be run. You can enter any value between 0 and 999 for the millisecond. This field is enabled only if you have selected **Add Test**.

Pane	Description
Apply the Monitoring Test	
Run the above monitoring test case	Check the checkbox to run the above monitoring test case.
Configure Syslog	Check the checkbox and select the following options to enable or disable Syslog: • Enable • Disable
Applicable Devices (Button)	Allows you to view the IOS devices in your selection that you want to monitor with GOLD Health Monitoring Tests.
Save (Button)	Saves the information you have specified.
Reset (Button)	Clears all fields and reverts to the default setting.
Cancel (Button)	Ignores your changes.

For more information, see *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1*.

SRE Operation Task

You can use the SRE Operation task to perform the following operations in the service modules of SRE supported devices:

- Install application in service modules
- Uninstall application from service modules
- Understand:
  - Status of the service module
  - Application that is running on the module
  - Status of the current installation in the service module
  - Status of uninstallation in the service module
- Stop the installation on a set of service modules in a SRE device
- Reset service modules in a SRE device
- Shutdown the set of service modules in a SRE device

You can enter the details of the SRE Operation task in the SRE Operation Configuration dialog box. To invoke this dialog box, see Create a NetConfig Job based on Module or Port.

The fields in the SRE Operation Configuration dialog box are:

Field	Description
Action	Select the following actions: • Install—Install application in service modules. • Uninstall—Uninstall application from service modules. • Status—Displays the following: – Status of the service module – The applicable running on the module – Status of the installation and uninstallation being performed in the service module • Abort—Stop installation on a set of service modules in a SRE device. • Shutdown—Shutdown the set of service modules in a SRE device • Reset—Reset service modules in a SRE device.
Script Name [Optional]	Name of the script file that should be picked up during installation. This field is optional and is enabled only if the Install action is selected.
Argument to the Script [Optional]	String argument passed to the script. The string argument must be entered within quotes. For example, “argument”. This field is optional and enabled only if Install action is selected.
URL of the installation source directory	URL path of the package from where the device needs to download the image for installation. For example, ftp://180.180.180.80/nibbler/012609/pkg1/foundation.sme.1.4.40.18.pkg This is a mandatory field. If this field is blank, an error message appears.
Applicable Devices	Allows you to view the devices in your selection that you want to configure SRE operation.
Save (Button)	Saves the information you have specified.
Reset (Button)	Clears all fields and reverts to the default setting.
Cancel (Button)	Ignores your changes.

cwcli netconfig

This command is described in the cwcli framework chapter. For details see Running the cwcli netconfig Command.

Use Case: Using NetConfig Templates to change Configurations for many Devices

Case

As a Network Administrator, you would want to change configuration for a set of devices in few simple steps.

Solution

You can use NetConfig to change the configurations of many devices in one step. You can select the devices and the corresponding system-defined or user-defined tasks and schedule a NetConfig job.

Let us say, you want to change the Local Username and Telnet password for a few devices. To perform this:

Step 1 Go to **Configuration > Configuration** > **NetConfig.**

The Devices And Tasks dialog box appears.

Step 2 Select the required devices from the Device Selector.

Step 3 Select the **Local Username** and **Telnet Password tasks** from the Task Selector.

NetConfig Tasks are also referred to as NetConfig templates.

Step 4 Click **Next**.

From your selection, only the tasks that are applicable to at least one device that you have selected, appear here. If the task that you have selected do not apply to the categories of any of the devices that you have selected, it will not be displayed in the Applicable Tasks pane.

Step 5 Select a task and click **Add** to create an instance for the task.

Step 6 After creating the instances, select the **Local Username_1** instance and click **View CLI** button to view the CLI commands that will be deployed onto the applicable and non applicable devices.

Alternatively, you can click **Edit** to edit the selected instance or click **Delete** to delete an instance. You can only delete one instance at a time.

Step 7 Click **Next**.

The Job Schedule and Options page appears.

For more information on how to schedule a NetConfig job, see Starting a New NetConfig Job.

Step 8 Provide the required information in the Job Schedule and Options dialog box and click **Finish**.

The Job Work Order screen appears.

Step 9 Click **Finish**.

A notification indicating the successful creation of a job appears.

Example

```
Job 1007 was created successfully.
```

The NetConfig job will be executed at the scheduled date and time. The Local Username Configuration and Telnet Password Configuration changes effected will be deployed on the selected applicable devices.

To know the status of the job scheduled, go to **Configuration > Configuration** > **NetConfig** > **NetConfig Jobs**.

CHAPTER 5

Archiving Configurations and Managing them using Configuration Archive

Configuration Archive maintains an active archive of the configuration of devices managed by LMS. It enables you to perform the following tasks:

- Fetch, archive, and deploy device configurations
- Search and generate reports on archived data
- Compare and label configurations, compare configurations with a baseline, and check for compliance.

You can also perform some of the Configuration Archive tasks using command line utility **`cwcli config`**.

You can also export the configuration data using the **`cwcli export config`** command.

See CLI Utilities for further details on **`cwcli config`** and **`cwcli export config`** commands.

This chapter gives information on performing Configuration Archive tasks (see Performing Configuration Archive Tasks for details).

This chapter contains:

Performing Configuration Archive Tasks

Configuration Archive allows you to:

- Check archival status

  You can check the overall status of the configuration archive (For example, Successful, Partially Successful, etc.).

  See Checking Configuration Archival Status for further details.

- Update the archive

  In addition to scheduling configuration archive update, you can also update the archive manually. This ensures that you have the latest configurations.

  See Scheduling Sync Archive Job for more details. To define the Configuration Collection Settings, see *Administration of Cisco Prime LAN Management Solution 4.1*.

- Determine Configuration Protocol usage details

  You can view the protocol usage details for successful configuration fetches for devices. You can also change the transport protocol order after analyzing the protocol usage trends.

  See Using the Config Fetch Protocol Usage Report for more details.

- Determine out-of-sync configuration files

  You can list the devices for which running configurations are out-of-sync- with the startup configuration.

  See Generating an Out-of-Sync Report and Scheduling Sync on Device Job for further details.

- View Version Tree

  You can view all configuration versions of selected devices in the form of a graphical display.

  See Using the Configuration Version Tree for further details.

- View Version Summary

  You can view the latest three archived configurations for selected devices. It also has a link to view a particular configuration running on the device and to generate differences between versions in the archive.

  See Viewing the Configuration Version Summary for further details.

- Search for device configuration files

  You can search the archive for configuration containing text patterns for selected devices.

  See Using Search Archive for further details.

- Create custom configuration queries (See Creating a Custom Query.)

  You can create and run custom queries that generate reports. These reports display device configuration files from the archive for the devices you specify. You can use custom queries while searching archives.

- Compare configurations

  You can compare the following:

  – Startup and running configurations

  – Running and latest archived configurations

  – Two configuration versions of the same device

  - Two configuration versions of different devices
  - Base configuration and latest version of different devices

  See Comparing Configurations for further details.

- Configuration Quick Deploy

  You can create an immediate job to deploy the version of configuration that you are viewing on the device. You can deploy the configuration either in the Overwrite or Merge mode. You can also use job-based password.

  See Configuration Quick Deploy for further details.

- Configuration Archive Job Browser

  You can see the status of your Configuration Archive jobs.

  See Using Configuration Archive Job Browser for further details.

- Label Configuration

  You can select configuration files from different managed devices and then group and label them.

  See Configuring Labels for further details.

- Set the debug mode for Configuration Archive

  You can set the debug mode for Configuration Archive feature in the Log Level Settings dialog box (**Admin > System > Debug Settings**).

  See *Administration of Cisco Prime LAN Management Solution 4.1* for more details.

Checking Configuration Archival Status

After you add devices, their configurations are gathered and stored in the configuration archive. You can check the overall status of the configuration archive (Successful, Partially Successful, and Failed). It provides the status of the last archival attempt.

Refresh (Icon)	Click on this icon to refresh the configuration archive status window.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To check the configuration archive status:

Step 1 Select **Configuration** > **Configuration Archive** > **Summary**.

The Configuration Archival Summary dialog window appears with the following information.

Archival Status	Description
Successful	Number of devices for which all supported configurations have been fetched successfully. Click **No.of Devices** to see the Successful Devices Report.
Failed	Number of devices for which fetch of all supported configurations has failed. Click **No.of Devices** to see the Failed Devices Report.
Partial Successful	Number of devices for which fetch of any one of the supported configurations has failed. Number of Catalyst 5000 devices for which sub-modules were not pulled into archive. Only the main configuration of supervisor engine module is archived for Catalyst 5000 devices. Click **No.of Devices** to see the Partially Successful Devices Report.
Configuration Never Collected	Number of devices for which the supported configurations has never been collected. Click **No.of Devices** to see the Configuration Never Collected Devices Report.

Step 2 Select one or all of the Config Archival Status and click **Sync Archive** to schedule an immediate job to update the archive status.

You can check the status of your scheduled *Sync Archive* job by selecting **Configuration > Job Browsers > Configuration Archive**.

Configuration Archival Reports

The following are the Config Archival reports:

- Successful Devices Report
- Failed Devices Report
- Partially Successful Devices Report
- Configuration Never Collected Devices Report

Successful Devices Report

A device appears in this report if all supported configurations have been fetched successfully.

Note These dates do not necessarily reflect when the archive was last updated.

This report contains the following information:

Column Names	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This config type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
File Type	Defines the configuration file type as either Running or Startup configuration.
Accessed At	Date and time at which LMS pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.
Description	Displays the archival status.

Failed Devices Report

A device appears in this report if fetch for all of the supported configurations has failed. This report also contains the reasons configuration could not be pulled.

This report contains the following information:

Column Names	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.
Config Type	Defines the type of configuration as PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains information about the Running and Startup configuration files. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
File Type	Defines the configuration file type as either Running or Startup configuration.
Accessed At	Date and time that LMS pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.
Description	Reason why LMS could not pull running and startup configuration from device.

If you have enabled TACACS for a device and configured custom TACACS login and passwords prompts, you may experience Telnet problems, since LMS may not recognize the prompts.

To make your prompts recognizable, you must edit the TacacsPrompts.ini file in:

- *NMSROOT*\objects\cmf\data\TacacsPrompts.ini (On Windows)
- *NMSROOT*/objects/cmf/data/TacacsPrompts.ini (On Solaris and Soft Appliance)

NMSROOT is the LMS install directory. For Solaris and Soft Appliance, it will be /opt/CSCOpx.

Partially Successful Devices Report

A device shows up in this report if fetch for any one of the supported configurations has failed.

The Partially Successful Devices report lists the Catalyst 5000 family devices for which sub-module information could not be pulled from the device. Only the main configuration of the supervisory module is archived for Catalyst 5000 devices.

This report contains the following information:

Column Names	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.
Config Type	Defines the type of configuration as PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
File Type	Defines the configuration file type as either Running or Startup configuration.
Accessed At	Date and time that LMS pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.
Description	Reason why LMS could not pull running or startup configuration from device.

Configuration Never Collected Devices Report

A device appears in this report if fetch for the supported configuration has never been collected.

This report contains the following information:

Column Names	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.
Config Type	Defines the type of configuration as PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
File Type	Defines the configuration file type as either Running or Startup configuration.
Accessed At	Date and time that LMS pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.
Description	Reason why LMS could not pull running or startup configuration from device.

Scheduling Sync Archive Job

You can schedule a job to update the configuration archive for a selected group of devices.

You have an option to poll device configuration before updating the archive and to fetch Startup configuration.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To schedule a job to update the device configuration:

Step 1 Select **Configuration > Configuration Archive > Synchronization**.

The Sync Archive dialog box appears.

Step 2 Select either:

- **Device Selector** — To schedule a job for a static set of devices.

  The sync archive job fails if devices are removed from the DCR. For example, a sync archive job is scheduled to run for all the devices that are part of the selected group in Device Selector. If a device, part of the selected group in Device Selector, is deleted from DCR while the job is running then the job fails for that particular device. However, the job succeeds for the remaining devices in the group, but the status of the job still remains failed.

Or

- **Group Selector** — To schedule a job for a dynamic group of devices.

  The job is scheduled only for the devices that are present in the selected group at the time when the job is run. The customizable group selector for jobs evaluates static groups also as dynamic during run time.

Step 3 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Sync Archive job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this task immediately. • 6 - hourly—Runs this task every 6 hours, starting from the specified time. • 12 - hourly—Runs this task every 12 hours, starting from the specified time. • Once—Runs this task once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the specified day of the week and at the specified time. • Monthly—Runs monthly on the specified day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule the job. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.
Job Information	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Job Options	
Poll device before configuration collection	Configuration Archive polls the device and compares the time of change currently on the device with the time of last archival of configuration to determine if configuration has changed on a device. If the polling is not supported on the device, then configuration fetch will be initiated without checking for the changes. See “Understanding Configuration Retrieval and Archival” section in *Administration Guide for Cisco Prime LMS 4.1* for further details on configuration polling.
Fetch startup config	Configuration Archive fetches the startup configuration.

Step 4 Click **Submit**.

A message appears, `Job` *ID* `is created successfully`.

Where *ID* is a unique Job number.

Step 5 Click **OK**.

You can check the status of your scheduled *Sync Archive* job by selecting **Configuration > Job Browsers > Configuration Archive**.

Using the Config Fetch Protocol Usage Report

You can view the configuration protocol usage details for successful configuration fetches using the Config Fetch Protocol Usage Report.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Select **Configuration** > **Configuration Archive > Protocol Usage Summary** to generate a Config Fetch Protocol Usage Report.

The Config Fetch Protocol Usage Report window displays the following information:

Column Name	Description
Protocol	Protocols used by LMS for configuration fetches.
Config Type	The Configuration types for the various protocols. The available types are: • Running — Count of the successful running configuration fetches for each protocol • Startup — Count of the successful startup configuration fetches for each protocol • VLAN — Count of the successful VLAN configuration fetches for each protocol. This configuration fetch is supported by only Telnet and SSH protocols. Click on the Count link to view a detailed report for a protocol and corresponding Config Type. The detailed report shows the list of devices which are accessed using a particular protocol and for which successful Config Fetch has happened. Example: If you click on a Count link, 20, for Telnet protocol and Running config type, a detailed report is generated with the following fields: • Device Name — Display name of each device. • Accessed At — Date and time at which each device was accessed for Config Fetch purpose. • Config Type — Configuration type for each device. • File Type -— Configuration file type for each device. This detailed report shows only the devices for which Telnet has successfully fetched configurations. You can use the export icon to export the list of devices from this detailed report to the device selector.

Column Name	Description
Edit Settings (Button)	Click this button, if you want to change the transport protocol order. For more information, see *Administration of Cisco Prime LAN Management Solution 4.1* for further details.
Refresh (Icon)	Refreshes the Config Fetch Protocol Usage Report.

Generating an Out-of-Sync Report

You can generate an Out-of-Sync report for the group of devices for which running configurations are not synchronized with the startup configuration.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Select **Configuration** > **Compliance** > **Out-of-Sync Summary** to generate an Out-of-sync report. The Startup and Running Out-Of-Sync Summary window displays the following information:

Column Name	Description
Device Name	Device Display Name as entered in Device and Credential Repository.
Startup	Startup configuration of the device. This configuration is fetched from the configuration archive. Click on the displayed date to view the configuration.
Diff	Difference between the archived Startup and archived Running configurations. Click on the icon to see the difference between the archived Startup and archived Running configurations.
Running	Running configuration of the device. This configuration is fetched from the configuration archive. Click on the displayed date to see detailed information on the Running configuration.
Sync on Device (Button)	Use this button to schedule a Sync on device job. You can schedule a Sync on device job to copy the running configuration of a device to the startup configuration. For more information see, Scheduling Sync on Device Job.

Scheduling Sync on Device Job

You can schedule a Sync on device job using the Sync on Device button on Startup and Running Out-Of-Sync Summary window.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To schedule a Sync on device job:

Step 1 Select **Configuration > Compliance** > **Out-of-Sync Summary**.

The Startup and Running Out-Of-Sync Summary dialog box appears.

Step 2 Select a device.

Step 3 Click **Sync on Device**.

The Job Schedule and Options dialog box appears.

Step 4 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Startup and Running Out-Of-Sync Summary report. To do this, select one of these options from the drop-down menu: • Immediate—Runs the report immediately. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the specified day of the week and at the specified time. • Monthly—Runs monthly on the specified day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule the job. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.
Job Information	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Approver Comments	Enter comments for the job approver. This field appears only if you have enabled Job Approval for Configuration Archive.
Maker E-Mail	Enter the e-mail-ID of the job creator. This is a mandatory field. This field appears only if you have enabled Job Approval for Configuration Archive.

Field	Description
Job Options	
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either: – Enter the device login user name and password and device Enable password or – Disable the Job Password option in the Job Schedule and Options dialog box.

Step 5 Click **Submit**.

A message appears, `Job` *ID* `is created successfully`.

Where *ID* is a unique Job number.

Step 6 Click **OK**.

You can check the status of your scheduled *Copy Running Config to Startup* job by selecting **Configuration > Job Browsers > Configuration Archive**.

Using the Configuration Version Tree

You can view all configuration versions of the selected devices in the form of a graphical display. You can also perform a configuration quick deploy for a selected device.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To view the configuration Version Tree:

Step 1 Select **Configuration > Configuration Archive > Views > Version Tree**

The Device Selection dialog box appears.

Step 2 Select a device. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 3 Click **OK**.

The Config Version Tree dialog box appears.

Step 4 Click either the configuration version which is a hyper link or select the radio button for the configuration version.

To expand the configuration version folder, click on the plus icon and select the configuration version to view the configuration.

The Config Viewer dialog box appears. See Understanding the Config Viewer Window for further information.

If you want to perform a configuration quick deploy (Configuration Quick Deploy), click the Deploy button.

Understanding the Config Viewer Window

The Config Viewer is a HTML-based window that displays the configurations of specified devices.

You can specify how you want to view the contents of the configurations by selecting one of the options under Show:

- Click **Raw** to view data exactly as it appears in the configuration file.
- Click **Processed** to view data with the commands ordered and grouped.

The Config Viewer window contains two columns.

Column	Description
Configlets	Click on any configlets to display the corresponding information. The available configlets vary from device to device; the following are examples: • All—Entire contents of the configuration files. • SNMP—SNMP configuration commands. For example, `snmp-server community public RO`. • IP Routing—IP routing configuration commands. For example, `router abcd 100`. • Interface folder—The different interface configuration commands. For example, `Interface Ethernet0` and `Interface TokenRing`. • Global—Global configuration commands. For example `no ip address`. • Line con 0—configuration commands for line console 0. • IP—IP configuration commands. For example, `ip http server`.
Configuration file name	View the contents of the configuration file.

The buttons on the Config Viewer are:

Button	Description
Download Config (Icon)	Downloads the configuration file to the client machine. This option to download the configuration file is available only in the Raw mode. The configuration file will be downloaded through the Web browser with the file name convention as *DeviceName-Version_Number*.txt. You can download the configuration file only if you have the privileges of a Network Administrator. **Note** The Credentials in the configuration file will be exposed and shown as clear text.
Export (Icon)	Export the configuration file. • If you are using the Raw mode then the exported file format is cfg. The file name convention is *DeviceName-VersionNumber*.cfg. • If you are using the Processed mode then the exported file format is XML. The file name convention is *DeviceName-VersionNumber*.xml. Where *DeviceName* is the device Display Name as entered in Device and Credential Repository and *VersionNumber* is the device configuration version. The default directory to which Configuration Archive file is exported is: On Solaris and Soft Appliance server, /var/adm/CSCOpx/files/rme/dcma/configexport On Windows server, *NMSROOT*\files\rme\dcma\configexport

Button	Description
Export (continue)	To export a file: 1. Click on the icon. The Export Config File dialog box appears. 2. Enter the folder name on the LMS server. You must enter the default export directory. You cannot enter any other directory. or Browse to select a folder on the LMSserver. The Server Side File Browser dialog box appears. a. Select a folder on the LMS server. b. Click **OK**. The Browse button takes you to the default directory. It does not allow you to change this default export directory. 3. Click **OK**. If you have exported configuration in the Raw mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*`.cfg` If you have exported configuration in the Processed mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*`.XML` Where *ExportedFolder* is the location where configuration file is exported. 4. Click **OK**.
Print (Icon)	Generates a format that can be printed.
Compare with previous version	Compares configuration with previous version. When you click on this button, a new window Config Diff Viewer opens to show configurations side by side. See Understanding the Config Diff Viewer Window for further details. This button gets activated only if you have a previous version of the configuration.
Compare with next version	Compares configuration with next version. When you click on this button, a new window Config Diff Viewer opens to show configurations side by side. See Understanding the Config Diff Viewer Window for further details. This button gets activated only if you have a next version of configuration.
Edit	Launches Config Editor window. This button is active only if you are viewing the configuration version from the archive. See Editing and Deploying Configurations Using Config Editor for further details.
Deploy	Perform a quick configuration deploy. This button is active only if you are viewing the configuration version from the archive. See Configuration Quick Deploy.

Viewing the Configuration Version Summary

You can view all archived configurations for selected devices. It also provides a link to view a particular configuration running on the device and to generate differences between versions in the archive.

You can view the last three configuration versions for each device regardless of the number of versions stored in the archive.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To view the Config Summary, follow this workflow:

Step 1 Select **Configuration > Configuration Archive > Views > Version Summary.**

The Device Selection dialog box appears.

Step 2 Select a device. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 3 Click **OK**.

The Summary of Archived Versions window appears with the information in Table 5-1.

Table 5-1 Fields in the Summary of Archived Versions Window

Column	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.
Config Type	Defines the type of configuration as PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
Startup	Configuration running when device was started. This configuration is fetched from the device. Click on the Startup icon to view the Startup configuration.
Diff	Differences between Startup and Running configurations. To view the difference between Startup and Running configurations, click on the Diff icon.
Running	Configuration currently running on device. Click on the Running icon to view the Running configuration. The configuration that appears, is fetched from the device. This happens if the fetched configuration is different from the latest configuration that is in the archive. Otherwise, the latest configuration from the archive appears.
Diff	Differences between the Running Configuration on the device and the most recent archived configuration. To view the difference between the two running configurations, click on the Diff icon.

Table 5-1 Fields in the Summary of Archived Versions Window (continued)

Column	Description
Latest	Displays date and time of most recent configuration archive. The time shown here is the time when the file was actually archived. If the file was archived on 03/07/2004 5.00 PM PST, that's the time that will appear in this report. Time will be shown based on the client's time zone. To view the device configuration, click on **Date** and **Time**. The Archived At fields that appear in other configuration reports shows the last time the configuration was taken from the device in an attempt to archive. The system archives the configuration only if there is a change in the newly obtained configuration when compared with the archived one. So there could be different time values.
Diff	Differences between the most recent and the second most recent archived configurations. To view the difference between the two running configurations, click on the Diff icon.
Latest-1	Date and time the second most recent configuration was archived. To view the device configuration, click on **Date** and **Time**.
Diff	Differences between the second most recent and third most recent configurations in archive. To view the difference between the two running configurations, click on the Diff icon.
Latest-2	Date and time the third most recent configuration was archived. To view the device configuration, click on **Date** and **Time**.

Configuration Quick Deploy

You can create an immediate job to deploy the version of configuration being viewed on the device. You can deploy the configuration either in overwrite or merge mode.

Features of Configuration Quick Deploy

The following are the features of Configuration Quick Deploy:

- It can be performed for both running and startup configurations of all categories of devices.
- The job is executed immediately. Therefore Job approval should not be enabled at the time of Configuration Quick Deploy.
- The jobs cannot be rolled back.
- The jobs use TFTP, Telnet, SSH, SCP, RCP, HTTPs transport protocols.
- It provides an option to select either merge or overwrite mode when you deploy configuration on a device.
- It cannot be performed for VLAN configurations. However, you can deploy VLAN configurations using the CLI command, `cwcli config put`. See Overview: cwcli config Command for more information.
- It is supported for configuration versions in the archive only. That is, you cannot deploy for configuration version available on a device.
- The jobs use the same protocol order that you have specified in the Config Transport Settings (**Admin > Collection Settings > Config > Config Transport Settings**).

Performing a Configuration Quick Deploy

You can perform a configuration quick deploy using the Config Viewer window.

For example, you can launch Config Viewer window by clicking on Startup configuration or Running Configuration links while performing tasks such as generating Out-Of-Sync Summary report, viewing the Version Summary report etc.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Click **Deploy** on the Config Viewer (Understanding the Config Viewer Window) window.

The Job Option Details dialog box appears.

Step 2 Enter the following information:

Field	Description
Job Information	
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Job Options	
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either: – Enter the device login user name and password and device Enable password or – Disable the Job Password option in the Job Schedule and Options dialog box.

Field	Description
Deploy Mode	
Overwrite	Select the Overwrite option, if you want to replace the existing running configuration on the device, with the selected configuration. This is the default option for the configuration deployment. The configuration that you have selected is compared with the latest running configuration in the Configuration Archive. (LMS assumes that the latest running configuration in the archive is the same as the configuration currently running on the device.) The Overwrite mode ensures that the running configuration on the device is overwritten with the selected configuration. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same.
Merge	Select the Merge option, if you want to add incremental configuration to the device. The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration. The selected running configuration is not compared with the running configuration in the Configuration Archive. We recommend that you use this option on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device.

Step 3 Click **Submit**.

An immediate Quick Deploy of Configuration on Device job will be scheduled.

A message appears, `Job` *ID* `is created successfully`.

Where *ID* is a unique Job number.

Step 4 Click **OK**.

You can check the status of your scheduled *Config Quick Deploy* job by selecting **Configuration > Job Browsers > Configuration Archive**.

What Happens During Configuration Quick Deploy

Before Configuration Management deploys the configuration on the device, it verifies whether the device is locked.

The deploy process follows the configured transport protocol order and the fallback option is active.

At end of this task, Configuration Management will:

- Unlock the device
- Check in the new version of configuration if the deploy completes successfully.

After uploading the configuration on the device, Configuration Management writes to the Change Audit log.

Configuring Labels

A label is a name given to a group of customized selection of configuration files. You can select configuration files from different devices, group and label them.

These labeled files are not purged along with the other configuration files. You have to explicitly select the Purge labeled files option to purge the labeled files. These labeled files are not purged if this option is not enabled.

You can purge the label config files using **Admin > Network > Purge Settings.**

See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for further details.

The Label Config window displays the following information:

Column	Description
Label Name	Displays the label name.
Description	Displays the label description.
Created by	Displays the user who created this label.
Created on	Displays the label creation time.

You can click on any column heading to sort the information by that column. If you double-click a heading, the order is reversed.

The Label Configs window contains the following buttons:

Button	Description
Create	Create a label. See Creating a Label for further details.
Edit	Edit a labeled configuration. See Editing a Labeled Configuration for further details. This button is active only after you select a Label.
View	View a labeled configuration. See Viewing the Labeled Configuration for further details. This button is active only after you select a Label.
Delete	Delete labeled configuration. See Deleting the Labeled Configuration for further details. This button is active only after you select a Label.

Creating a Label

You can use Label Configuration to create a group of configuration files from selected devices.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

You can create a label file using the following workflow:

Step 1 Select **Configuration > Configuration Archive > Label Configs**.

The Label Configs dialog box appears.

Step 2 Click **Create**.

The Device Selection dialog box appears.

Step 3 In Device Selector pane, select the devices. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 4 Go to the Label selection pane and:

- Enter the Label Name. You can enter up to 64 characters.
- Enter the Label Description. You can enter up to 128 characters.

Step 5 Go to the Config Type pane and select Primary or VLAN.

Option	Description
Primary	Contains the Running and Startup configuration files information.
VLAN	Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information.

Step 6 Go to the Version pane and select **Latest** to include the most recent configuration only, or **All** to view all configuration versions.

- If you have selected Latest, you can click **Finish** button in the Select Devices page and complete the Label creation.
- If you have selected All, go to Step 7.

Step 7 Click **Next**.

The Select Configs to be Labelled dialog box appears.

- To view the configuration, select a configuration version file from the left pane and click **View**. The Config Viewer (Understanding the Config Viewer Window) window appears.
- To add the selected configuration, select a configuration version file from the left pane and click **Add**.
- To remove the selected configuration, select a configuration version file from the right pane and click **Remove**.

Step 8 Click **Finish**.

A message appears, `Label` *LabelName* `created successfully`.

Where *LabelName* is the name of the label that you entered.

Step 9 Click **OK**.

Editing a Labeled Configuration

You can make the following changes to a label:

- Modify the Label Description.
- Remove configuration files from the Selected Versions list.
- Add new configuration files from the Devices list.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

You can edit a label file using the following workflow:

Step 1 Select **Configuration > Configuration Archive > Label Configs**.

The Label Configs dialog box appears.

Step 2 Select a label and click **Edit**.

The Device Selection dialog box appears. The devices that are already part of the labeled file are selected.

Step 3 Go to the Device Selector pane and select a new device or deselect a device. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 4 Go to the Version pane and select **Latest** to include the most recent configuration only, or **All** to view all configuration versions.

Step 5 Click **Next**.

The Label Details dialog box appears with the current details of the label.

Step 6 Do either of the following:

- Change the Label Description. You can enter up to 128 characters.
- Select a configuration version file from the left pane, click **Add** to add the selected configuration file.
  - If you selected **Latest** in the previous dialog box, the left pane will show devices and the latest archived configuration file. The right pane contains labeled configuration.
  - If you selected **All** in the previous dialog box, the left pane will show devices and all available archived configuration files. The right pane contains labeled configuration.

Note You can select only one configuration file for a device.

- To remove the selected configuration, select a configuration version file from the right pane and click **Remove**.
- To view the configuration, select a configuration version file from the left pane and click **View**. The Config Viewer (Understanding the Config Viewer Window) window appears.

Step 7 Click **Finish**.

A message appears, `Label` *LabelName* `updated`.

Where *LabelName* is the name of the label as entered by you.

Step 8 Click **OK**.

Viewing the Labeled Configuration

You can view configurations of a label from the label listing.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Configuration Archive > Label Configs**.

The Label Configs dialog box appears.

Step 2 Select a label and click **View**.

The Label Config Viewer window appears with the following information:

Column Name	Description
Device Name	Device Display Name as entered in Device and Credential Repository.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
Version	Version of configuration file. Click on the version to display Config Viewer (see Understanding the Config Viewer Window), which shows contents of corresponding configuration file. In the Config Viewer window, you can click the Deploy button if you want to perform a Configuration Quick Deploy (Configuration Quick Deploy)
Created On	Date and time at which configuration file was created.
Change Description	Description of the configuration change.

Deleting the Labeled Configuration

You can delete a label from the list of labels in the label configuration dialog box:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Configuration Archive > Label Configs**.

The Label Configs dialog box appears.

Step 2 Select the labels and click **Delete**.

A message appears, `Are you sure you want to delete the label(s)?`

Step 3 Click **OK** to delete the labels.

Using Search Archive

You can search the archive for configuration containing text patterns for selected devices. You can specify ten different combinations of patterns or strings as part of search criteria.

For example:

- Search all devices for configurations having pattern **`set banner motd`** and **`set banner exec`**.
- Search all devices for configurations having pattern **`set banner motd`** and **`set banner exec`** and **`set password`**.

You can also specify an option to ignore or consider the case sensitive property.

You can create a custom configuration query that searches information about the specified configuration files.

If you monitor devices X, Y, and Z every morning, you can create a custom query on them. When you run the query, LMS quickly gathers all the archived configuration files for these devices and displays them in a report.

The Custom Queries window displays the following information:

Column	Description
Query Name	Custom Query name.
Description	Custom Query description.
Created By	User who created this Custom Query.
Created On	Custom Query creation time.

You can click on any column heading to sort the information by that column. If you double-click a heading, the order is reversed.

The Custom Queries window contains the following buttons:

Button	Description
Create	Create a custom query. See Creating a Custom Query for further details.
Edit	Edit a custom query. See Editing a Custom Query for further details. This button is active only after you select a custom query.
Run	Run a custom query. See Running a Custom Query for further details. This button is active only after you select a custom query.
Delete	Delete custom queries. See Deleting the Custom Queries for further details. This button is active only after you select a custom query.

The user who creates the custom query has full permission to perform tasks such as edit and run on the Custom Queries.

See Searching Archive for the procedure to search the configuration with and without a search pattern.

Creating a Custom Query

To create a custom query:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Configuration Archive > Views > Custom Queries**.

The Custom Queries dialog box appears

Step 2 Click **Create**.

Step 3 Do any of the following:

- Enter the Custom Query name. You can enter up to 64 characters.
- Enter the Custom Query description. You can enter up to 128 characters.
- Enter patterns to search for, for example, http server. You can enter text patterns up to 64 characters.

  To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields. You can specify ten different combinations of patterns as part of search criteria.

  You cannot search for special characters or regular expressions, for example, Control-C, boot*, etc.
- Select the search criteria **Contains**/**Does Not Contain**.
- If you have entered string as a search pattern, you can select **Match Any** to search for any given pattern string or **Match All** to search for all pattern strings.
- Click **Match Case** to perform a case-sensitive search, which is more efficient when you know the exact pattern you want to match. By default, Match Case is disabled.

Step 4 Click **OK**.

A message appears, `Custom Query` *CustomQueryName* `created successfully`.

Where *CustomQueryName* is the name of the custom query as entered by you.

Step 5 Click **OK**.

Running a Custom Query

To run a custom query:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Configuration Archive > Views > Custom Queries**.

The Custom Queries dialog box appears.

Step 2 Select a Custom Query and click **Run**.

The Device Selection dialog box appears.

Step 3 Select the devices. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 4 Click **OK**.

The Custom Query Search Result window appears with the following information:

Column Name	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.
Version	Versions of configuration file. Click on the version to display Config Viewer (see Understanding the Config Viewer Window), which shows contents of corresponding configuration file. In the Config Viewer window, you can click on the Deploy button if you want to perform a configuration quick deploy (Configuration Quick Deploy)
Created On	Date and time at which the configuration file was created.

You can perform the following tasks from this window:

- Select the devices and click **NetConfig** to make any changes to the device configuration using NetConfig templates.
- Select a device and click **Edit** to edit the device configuration using the Config Editor application.

Editing a Custom Query

You can edit the Custom Query description and modify the search patterns and their criteria. To edit a custom query:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Configuration Archive > Views > Custom Queries**.

The Custom Queries dialog box appears.

Step 2 Select a Custom Query and click **Edit**.

The Custom Query Window appears.

Step 3 Do any of the following:

- Update the Custom Query description. You can enter up to 128 characters.
- Either add a new search pattern or delete or update an existing search pattern and its criteria. You can enter up to 64 characters.
- Modify the string search option Match Any to Match All or vice versa.
- Enable or Disable the case-sensitive search.

Step 4 Click **OK**.

A message appears, `Custom Query` *CustomQueryName* `updated successfully`.

Where *CustomQueryName* is the name of the Custom Query.

Step 5 Click **OK**.

Deleting the Custom Queries

To delete the custom queries:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Configuration Archive > Views > Custom Queries**.

The Custom Queries dialog box appears.

Step 2 Select a Custom Query and click **Delete**.

A message appears, `The query will be deleted`.

Step 3 Click **OK**.

Searching Archive

You can search the device configuration file with or without the search pattern. You can also narrow down your search using Label Configuration files and Custom Queries.

You can view the search report in two ways:

- Search Archive Result
- Device Configuration Quick View Report

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To search the configuration archive:

Step 1 Select **Configuration > Configuration Archive > Views > Search Archive**.

The Search Archive dialog box appears.

Step 2 Enter the following:

Field	Description
Left Pane	
Label Config	Enable this option and select a label name. The configuration version options Latest and All are disabled.
Device Selector	Select the devices. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector. If you have selected Label Config, you need not select devices. If you have selected any devices, only the devices that are specified in the label configuration are searched. Other devices are ignored.
Version	Select **Latest** to search the most recent configuration only or **All** to search all configuration versions. If you have selected Label Config, then you cannot specify the versions.
View Type	Select one of these view types: • **Version** to view the Device Configuration Version Report. This displays all versions of the configuration, the time and date the configurations were archived, and reason for archival. • **Quick View** to view the Device Configuration Quick View Report. This displays the contents of the configuration files.
Right Pane	
Custom Query	Select a Custom Query. The search patterns that are defined in the Custom Query appear in the Pattern Details text boxes. In addition to Custom Query search patterns, you can also add additional search patterns.

Field	Description
Pattern Details	Perform the following tasks: • Enter patterns to search for, for example, *http server*. You can enter text patterns up to 64 characters. To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields. You can specify ten different combinations of patterns as part of search criteria. You cannot search for special characters, for example, *Control-C, boot**. You can also search the device configuration file without the search pattern. The search will list all archived configuration for all selected devices. – If you have selected the version as **Latest,** the search will list latest archived configuration for all selected devices. – If you have selected the version as **All,** the search will list all archived configurations for all selected devices • Select the search criteria **Contains**/**Does Not Contain**. • If you have entered string as a search pattern, you can select **Match Any** to search for any given pattern string or **Match All** to search for all pattern strings • Click **Match Case** to perform a case-sensitive search, which is more efficient when you know the exact pattern you want to match. By default, Match Case is disabled.
Date Range	Select any of the following Date Range types: • **As on**—Search config archives on or before the specified date and time. • **From**—Search config archives for the specified period. • **Last**—Search config archives for the last *N* number of days, weeks, months or years; where *N* is the value entered for the number of days, weeks, months or years. The following maximum values for *N* can be specified: – Days—The maximum number of days that can be specified is 999. – Weeks—The maximum number of weeks that can be specified is 999. – Months—The maximum number of months that can be specified is 99. – Years—The maximum number of years that can be specified is 9. If you have selected **Latest** as the version, the Date Range option searches for the most recent config archives.

Step 3 Click **Search**.

Based on your View type selection, either Search Archive Result or Device Configuration Quick View Report appears.

Search Archive Result

The Search Archive Result displays information about the device configurations. The Search Archive Result contains the following details of the selected configurations:

Column Name	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This config type does not contain Startup configuration file information. For ONS devices, the PRIMARY config type displays the configuration information from the active CPU, at that instance.
Version	Versions of configuration file. Click on the version to display Config Viewer (see Understanding the Config Viewer Window), which shows contents of the corresponding configuration file.
Created On	Date and time at which the configuration file was created.
Change Description	Cause of configuration change.

You can perform the following tasks from this window:

- Select the devices and click **NetConfig** to make changes to the device configuration using NetConfig templates.
- Select a device and click **Edit** to edit the device configuration using the Config Editor application.

Device Configuration Quick View Report

The Device Configuration Quick View report lists the devices, configuration version numbers, and configuration details of the device configuration version you specified.

You can specify how you want to view the contents of the configurations by selecting one of the options under Show:

- Click **Raw** to view data exactly as it appears in the configuration file. There are two panes, one lists all devices and the other displays the configuration.
- Click **Processed** to view data with the commands ordered and grouped. There are three panes, one lists all devices, the second pane lists all configlets, and the third pane displays the configuration.

Column	Description
Devices	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Troubleshooting page.
Configlets	You can click on any configlets to display the corresponding information. The available configlets vary from device to device. The following are examples: • All—The entire contents of the configuration files. • SNMP—SNMP configuration commands. For example, `snmp-server community public RO`. • IP Routing—IP routing configuration commands. For example, `router abcd 100`. • Interface folder—The different interface configuration commands. For example, `Interface Ethernet0` and `Interface TokenRing`. • Global—Global configuration commands. For example `no ip address`. • Line con 0—Configuration commands for line console 0. • IP—IP configuration commands. For example, `ip http server`.
Configuration file name	You can view the contents of configuration file.

The following buttons are available on the Config Viewer:

Button	Description
Export (Icon)	Exports the configuration file. • If you are using the Raw mode then the exported file format is cfg. The file name convention is *DeviceName-VersionNumber*.cfg. • If you are using the Processed mode then the exported file format is XML and the file name convention is *DeviceName-VersionNumber*.xml. Where *DeviceName* is the device Display Name as entered in Device and Credential Repository and *VersionNumber* is the device configuration version. The default directory where Configuration Archive file is exported is: On Solaris and Soft Appliance server, /var/adm/CSCOpx/files/rme/dcma/configexport On Windows server, *NMSROOT*\files\rme\dcma\configexport

Button	Description
Export (continue)	To export a file: 1. Click on the icon. The Export Config File dialog box appears. 2. Enter the folder name on the LMS server. You must enter the default export directory. You cannot enter any other directory. or Browse to select a folder on the LMS server. The Server Side File Browser dialog box appears. a. Select a folder on the LMS server. b. Click **OK**. The Browse button takes you to the default directory. The Server Side File Browser does not allow you to change this default export directory. 3. Click **OK**. If you have exported configuration in the Raw mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*`.cfg` If you have exported configuration in the Processed mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*`.XML` Where *ExportedFolder* is the location to which the configuration file is exported. 4. Click **OK**.
Print (Icon)	Generates a format that can be printed.
Compare with previous version	Compares configuration with the previous version. When you click on this button, a new window Config Diff Viewer opens to show configurations side by side. See Understanding the Config Diff Viewer Window for further details. This button is active only if you have a previous version of configuration.
Compare with next version	Compares configuration with the next version. When you click this button, a new window Config Diff Viewer opens to show configurations side by side. See Understanding the Config Diff Viewer Window for further details. This button is active only if you have a next version of configuration.
Edit	Launches Config Editor window. This button is active only if you are viewing the configuration version from the archive. See Editing and Deploying Configurations Using Config Editor for further details.
Deploy	You can perform a configuration quick deploy. This button is active only if you are viewing the configuration version from the archive. See Configuration Quick Deploy.

Comparing Configurations

You can compare two device configuration files from version to version or from device to device. You can also compare the configuration when a device was started with the current configuration, and the current configuration with the most recently archived configuration.

You can list the commands that have to be excluded while comparing configurations.

To do this select **Admin > Collection Settings > Config > Config Compare Exclude Commands Configuration.**

You can compare the configurations in these ways:

- Startup vs. Running—Compares the configuration when the device was started with the current configuration. These configurations are fetched from the device.

  See Comparing Startup vs. Running Configurations.

- Running vs. Latest Archived—Compares the running configuration with the most recently archived configuration. The Running configuration is fetched from the device.

  See Comparing Running vs. Latest Archived Configurations.

- Two Versions of the Same Device—Compares two archived configuration versions.

  See Comparing Two Configuration Versions of the Same Device.

- Two Versions of Different Devices—Compares any two configurations in the configuration archive.

  See Compare Two Configuration Versions of Different Devices.

- Base Config vs. Latest Version of Different Devices—Compares the base configuration of a device with the latest configuration of other devices.. These configurations are fetched from the device.

  See Compare Base Config vs. Latest Configuration Version of Multiple Devices.

Comparing Startup vs. Running Configurations

You can compare the configuration when a device was started with the current configuration. These configurations are fetched from the device.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To compare Startup vs. Running configurations:

Step 1 Select **Configuration > Configuration Archive > Compare Configs**.

The Compare Configurations dialog box appears.

Step 2 Select **Startup vs. Running** and click **Compare**.

The Device Selection dialog box appears.

Step 3 Select a device. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 4 Click **OK**.

The Understanding the Config Diff Viewer Window window appears.

Comparing Running vs. Latest Archived Configurations

You can compare the configuration currently running on a device with the most recent configuration stored in the configuration archive. The Running configuration is fetched from the device.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To compare Running vs. latest archived configurations:

Step 1 Select **Configuration > Configuration Archive > Compare Configs**.

The Compare Configurations dialog box appears.

Step 2 Select **Running vs. Latest Archived** and click **Compare**.

The Device Selection dialog box appears.

Step 3 Select a device. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 4 Click **OK**.

The Understanding the Config Diff Viewer Window window appears.

Comparing Two Configuration Versions of the Same Device

You can compare two different archived configurations of the same device.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To compare two versions of the same device:

Step 1 Select **Configuration > Configuration Archive > Compare Configs**.

The Compare Configurations dialog box appears.

Step 2 Select **Two Versions of the Same Device** and click **Compare**.

The Device Selection dialog box appears.

Step 3 Select a device. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 4 Click **Next**.

The Select First Configuration dialog box appears with the following information:

Column Name	Description
Config Version	Versions of configuration file.
File Type	Defines the configuration file type as either Running or Startup configuration.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
Created On	Date and time at which the configuration file was created.

Step 5 Click on the first configuration to compare and click **Next**.

The Select Second Configuration dialog box appears with the same information as the Select First Configuration window.

Step 6 Click on the second configuration to compare it with first configuration and click **Finish**.

The Understanding the Config Diff Viewer Window window appears.

Compare Two Configuration Versions of Different Devices

You can compare two archived versions of a configuration of the same or different devices.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To compare two versions of different devices:

Step 1 Select **Configuration > Configuration Archive > Compare Configs**.

The Compare Configurations dialog box appears.

Step 2 Select **Two Versions of Different Devices** and click **Compare**.

The Select Device and Pattern dialog box appears.

Step 3 Perform the following and click **Next**:

Field	Description
Left Pane	
Device Selector	Select the devices. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.
Version	Select **Latest** to view the most recent configuration or **All** to view all configuration versions.
Right Pane	
Pattern Details	Perform the following tasks: 1. Enter patterns to search for, for example, http server. You can enter text patterns up to 64 characters. To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields. You can specify ten different combinations of patterns as part of search criteria. You cannot search for special characters or regular expressions, for example, Control-C, boot*. You can search the device configuration file without the search pattern. 2. Select the search criteria **Contains**/**Does Not Contain**. If you have entered string as a search pattern, you can select **Match Any** to search for any given pattern string or **Match All** to search for all pattern strings. 3. Click **Match Case** to perform a case-sensitive search, which is more efficient when you know the exact pattern you want to match. By default, Match Case is disabled.

The Select First Configuration dialog box appears with the following information:

Column Name	Description
Device Name	Device Display Name as entered in Device and Credential Repository.
Config Version	Versions of configuration file.
File Type	Defines the configuration file type as either Running or Startup configuration.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
Created On	Date and time at which the configuration file was created.

Step 4 Click on the first configuration to compare and click **Next**.

The Select Second Configuration dialog box appears with the same information as the Select First Configuration window.

Step 5 Click on the second configuration to compare with first configuration and click **Finish**.

The Understanding the Config Diff Viewer Window window appears.

Compare Base Config vs. Latest Configuration Version of Multiple Devices

You can compare and sync the base configuration of a device with the latest configuration version of multiple devices. The base configuration can be Running, Startup, or User archives.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To compare the base configuration with the latest configuration version of different devices:

Step 1 Select **Configuration > Configuration Archive > Compare Configs**.

The Compare Configurations dialog box appears.

Step 2 Select **Base Config vs. Latest Version of Multiple Devices** and click **Compare**.

The Select a Base Device dialog box appears.

Step 3 Select a base device. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 4 Click **Next**.

The Select Config Version of the Base Device to Compare dialog box appears.

Step 5 Select the configuration version of the base device from the Config Version tree.

- If you check **Filter Same Device Category Devices**, it displays devices that belong to the base device category. These devices are displayed in the Select Other Devices to Compare page.
- If you uncheck **Filter Same Device Category Devices**, it displays all devices that belong to other device categories that are managed by LMS. These devices are displayed in the Select Other Devices to Compare page.

Step 6 Click **Next**.

The Select Other Devices to Compare dialog box appears.

Step 7 Select the devices to compare with the configuration of the base device.

You can select devices using the Device Selector. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 8 Click **Next**.

The Add Exclude Commands dialog box appears

Step 9 Do the following in the Add Exclude Commands dialog box:

Field/Button	Description

Exclude Commands	Enter the exclude commands one in each line.
	For example,
	`ip address.*,`
	`end.*,`
	`exec-timeout.*,`
	`length.*,`
	`ntp clock-period.*`
	The commands will be excluded while comparing configuration.
	You can enter multiple commands separated by commas.
	For more information, see Examples for Exclude Commands.

View Base Config (Button)	Click **View Base Config** to launch the Config Viewer window. See Understanding the Config Viewer Window for further information.

Step 10 Click **Finish**.

The Compare Config window appears, displaying the following details:

Field Name/Buttons	Description
Summary	
Total No.of Device(s) selected for comparison	Number of devices selected for comparision.
Number of Compliant devices	Number of devices that comply with the base configuration.
Number of Non-Compliant devices	Number of devices that do not comply with the base configuration.
Number of Excluded devices	Number of devices excluded from comparision.
Base Device	Name of the base device.
Base Config Type	Configuration type of the base device.
Base Config Branch	Configuration branch version of the base device. For example, DeviceArchive.
Non-Compliant Devices	
Device Name	Device Display Name as entered in Device and Credential Repository.
Latest Version	Version of configuration file against which the compliance was checked. Click on the version to display Config Viewer (see Understanding the Config Viewer Window). This shows the contents of corresponding configuration file against which the compliance was checked.
Diff	Differences between base configuration and the lastest configuration version of mutiple devices. To view the difference between the base configuration and the latest configuration version of other devices, click on the Diff icon. The Config Diff Viewer window appears. For more information, see Understanding the Config Diff Viewer Window.

Field Name/Buttons	Description
Excluded Devices	
Device Name	Device Display Name as entered in Device and Credential Repository.
Reason for Exclusion	Displays the cause for exclusion.
Buttons	
Export (Icon)	Exports the data to a file of PDF or CSV format.
Print (Icon)	Generates a format that can be printed.

Step 11 Click **Diff** to view the differences between base configuration and the lastest configuration version of multiple devices.

The Config Diff Viewer window appears. For more information, see Understanding the Config Diff Viewer Window.

Step 12 Click **Deploy** to sync the base configuration with the latest configuration.

The Job Options Details pop-up window appears, displaying the following details:

Field	Description
Job Information	
E-mail	Enter the e-mail address.
Retain new config additions in <<config version>>	Check to retain new config additions in the configuration file.
Job Options	
Job Password	Check to enable Job Password option
Login username	Enter the login username.
Password	Enter the login password.
Enable password	Enter the enable password.
Submit (button)	Click **Submit** to run the job.

Step 13 Enter the Job Information and Job Option details.

Step 14 Click **Submit** to run the job.

Examples for Exclude Commands

This section contains examples for exclude commands:

Scenario	Command Type (Examples)
To exclude anything after IP Address	ip address .*
To exclude IP address range from 172.20.115.1 to 255	ip address 172\\.20\\.115\\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?) 255.255.255.128
To exclude SNMP host that contain either inside or outside characters	snmp host \\b(inside|outside) 10.77.203.176 community public

For more information, see the regex API guide for Java 1.4.2 from Oracle http://download.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html for other patterns.

Understanding the Config Diff Viewer Window

The Configuration Version Compare report shows the differences between the two selected configurations. You can access the Configuration Version Compare report by comparing device configurations.

You can specify how you want to view the differences between the configurations by selecting one of the options under Show:

- Click **Raw** to view the differences between the two raw configurations.
- Click **Processed** to view the differences with the commands ordered and grouped.

The color conventions that are used on Config Diff Viewer are:

- Black—All unchanged text.
- Red—Lines that have changed from one version to another.
- Blue—Lines that have been added or deleted from one of the versions.

The Configuration Versions Compare report has three columns:

Column	Description
Configlets	You can click on any configlet to display the corresponding information. The available configlets vary from device to device. The following are examples: • Diffs—Displays the differences between the two configuration files (if you selected more than one). • All—The entire contents of the configuration files. • SNMP—SNMP configuration commands. For example, `snmp-server community public RO`. • IP Routing—IP routing configuration commands. For example, `router abcd 100`. • Interface folder—The different interface configuration commands. For example, `Interface Ethernet0` and `Interface TokenRing`. • Global—Displays global configuration commands. For example `no ip address`. • Line con 0—Displays configuration commands for line console 0. • IP—Displays IP configuration commands. For example, `ip http server`.
First configuration file	Contains the contents of the first configuration file.
Second configuration file	Contains the contents of the second configuration file.

The buttons on the Config Diff Viewer are:

Button	Description
Export (Icon)	Export the configuration file. • If you are using the Raw mode then the exported file format is cfg. The file name convention is *DeviceName-VersionNumber*.cfg. • If you are using the Processed mode then the exported file format is XML. The file name convention is *DeviceName-VersionNumber*.xml. Where *DeviceName* is the device Display Name as entered in Device and Credential Repository and *VersionNumber* is the device configuration version. The default directory where Configuration Archive file is exported is: On Solaris and Soft Appliance server, /var/adm/CSCOpx/files/rme/dcma/configexport On Windows server, *NMSROOT*\files\rme\dcma\configexport

Button	Description
Export (continue)	To export a file: 1. Click on the icon. The Export Config File dialog box appears. 2. Enter the folder name on the LMS server. You must enter the default export directory. You cannot enter any other directory. or Browse to select a folder on the LMS server. The Server Side File Browser dialog box appears. a. Select a folder on the LMS server. b. Click **OK**. The Browse button takes you to the default directory. It does not allow you to change this default export directory. 3. Click **OK**. If you have exported configuration in the Raw mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*`.cfg` If you have exported configuration in the Processed mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*`.XML` Where *ExportedFolder* is the location where configuration file is exported. 4. Click **OK**. This option is not available in the Config Diff Viewer page when you compare Base Config vs. Latest Version of Different Devices.
Print (Icon)	Generates a format that can be printed. This option is not available in the Config Diff Viewer page when you compare Base Config vs. Latest Version of Different Devices.

Using Configuration Archive Job Browser

You can browse the Configuration Archive jobs that are registered on the system. From the Archive Management Jobs dialog box you can also retry, delete, stop jobs and view a job's details.

This section details:

- Retrying a Config Job
- Stopping a Config Job
- Deleting the Config Jobs
- Viewing the Configuration Archive Job Details

The Archive Management Jobs window displays the following information:

Column Name	Description
Job ID	Unique number assigned to the job when it is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001. Click on the Job ID to view the Configuration Archive job details (see Viewing the Configuration Archive Job Details).
Job Type	Type of the configuration job. • Sync Archive—Appears if you had scheduled a Sync Archive job (**Configuration > Configuration Archive > Synchronization**). • Get Config—Appears if you had scheduled a configuration fetch job using the CLI command, `cwcli config get`. • Put Config—Appears if you had scheduled a configuration retrieve job using the CLI command, `cwcli config put`. • Import Config—Appears if you had scheduled a job that retrieved the configuration from a file and if you had transferred it to the device using the CLI command, `cwcli config import`. • Write to Running Config—Appears if you had scheduled a job that downloaded the differences between the specified configuration file and the latest configuration version in the archive for the specified device, using the CLI command, `cwcli config write2run`.

Column Name	Description
Job Type (Continue)	• Write to Startup Config—Appears if you had scheduled a job that erased the contents of the device Startup configuration and if you wrote contents of a specified file as new Startup configuration, using the CLI command, `cwcli config write2start`. • Copy Running Config to Startup—Appears if you had scheduled a job that overwrote with the Startup configuration of the device with the Running configuration, using the CLI command, `cwcli config run2start`. • Copy Startup Config to Running—Appears if you had scheduled a job that merged the Startup configuration with the Running configuration, using the CLI command, `cwcli config start2run`. • Reload Device—Appears if you had scheduled a job that rebooted the devices, using the CLI command `cwcli config reload`. • Config Quick Deploy—Appears if you had created an immediate Configuration Quick Deploy job, using the Config Viewer window. • Compliance Check—Appears if you had scheduled a Compliance Check job (**Configuration > Compliance > Compliance Templates > Compliance Check** and click the Compliance Check button). • Check Compliance and Deploy—Appears if you had scheduled a Compliance Check job with the job option, Check compliance and deploy enabled (**Configuration > Compliance > Compliance Templates > Compliance Check** and click the Compliance Check button). • Deploy Baseline template—Appears if you had scheduled a Baseline Template deploy job (**Configuration > Compliance > Compliance Templates > Direct Deploy** and click the Deploy button). • Deploy Compliance Results—Appears if you had scheduled a Deploy job on the non-complaint devices (**Configuration > Compliance > Compliance Templates > Jobs** and click the Deploy button).
Status	Job states: • Cancelled—Running job stopped by you. • Failed—Failed job. Click on the Job ID to view the job details. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed is 5. • Running—Job still running. • Scheduled—Job scheduled to run. • Rejected—Job rejected by an approver. Click on the Job ID to view the rejection details. • Successful—Job completed successfully • Waiting for Approval—Job waiting for approval.
Description	Job description entered during job definition
Owner	User who created this job.
Scheduled at	Date and time at which the job is scheduled to run.
Completed at	Date and time at which job was completed.
Schedule Type	Run type of the job: Immediate, Once, 6 - hourly, 12 - hourly, Daily, Weekly, and Monthly.

You can click on any column heading to sort information by that column. If you double-click on a heading, the order is reversed.

You can use the Filter button to do a quick search on the Configuration Archive jobs. You can perform filters by using these options:

Filter Options	Description
Job ID	Unique number assigned to the job when it is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001.
Job Type	Types of Configuration Archive jobs. For example: Sync Archive, Write to Running Config.
Status	Status of the job. For example: Successful, Failed.
Description	Job description.
Owner	Owner of the job.
Schedule Type	Job schedule Type. For example: Immediate, Weekly.
Refresh (Icon)	Click on this icon to refresh the Configuration Archive Job Browser.

You can perform the following tasks on this window:

- Retrying a Config Job
- Stopping a Config Job
- Deleting the Config Jobs

Retrying a Config Job

You can retry only a failed job. You cannot retry a job that is scheduled to run periodically (Daily, Weekly, and Monthly).

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To retry a job:

Step 1 Select **Configuration > Job Browsers > Configuration Archive**.

The Archive Management Jobs dialog box appears.

Step 2 Select a failed job and click **Retry**.

The Job Schedule and Options dialog box appears.

Step 3 Enter the following information:

Based on your retry job selection, some of the options may not be visible.

For example, 6 - hourly and 12 -hourly Run Type options are visible only if you are retrying a Sync Archive job. This is not visible for other types of Configuration Archive jobs.

Field	Description
Scheduling	
Run Type	You can specify when you want to run the selected Retry job. To do this, select one of these options from the drop-down menu: • 6 - hourly—Runs this task every 6 hours, starting from the specified time. • 12 - hourly—Runs this task every 12 hours, starting from the specified time. • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the specified day of the week and at the specified time. • Monthly—Runs monthly on the specified day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not been completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) at which to schedule a job. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.

Field	Description
Job Information	
Approver Comments	Enter comments for the job approver. This field appears only if you have enabled job approval for Configuration Archive.
Maker E-Mail	Enter the e-mail-ID of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Configuration Archive.
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) either: – Enter the device login user name and password and device Enable password Or – Disable the Job Password option in the Job Schedule and Options dialog box.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). When the job starts or completes, an e-mail is sent with the LMS e-mail ID as the sender's address.

Step 4 Click **Submit**.

A message appears, `Job resubmitted successfully`.

Step 5 Click **OK**.

Stopping a Config Job

You can stop the following running job types (See Using Configuration Archive Job Browser for details on the job types):

- Put Config
- Import Config
- Write to Running Config
- Write to Startup Config
- Copy Running Config to Startup
- Copy Startup Config to Running
- Reload Device

- Config Quick Deploy
- Check Compliance and Deploy
- Deploy Baseline template
- Compliance check

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To stop an Configuration Archive job:

Step 1 Select **Configuration > Job Browsers > Configuration Archive**.

The Archive Management Jobs dialog box appears.

Step 2 Select a running job and click **Stop**.

A message appears, `Selected job(s) will be stopped`.

Step 3 Click **OK**.

Deleting the Config Jobs

You can delete jobs with status:

- Cancelled
- Failed
- Scheduled
- Rejected
- Successful
- Waiting for Approval

You cannot delete a running job.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To delete jobs:

Step 1 Select **Configuration > Job Browsers > Configuration Archive**.

The Archive Management Jobs dialog box appears.

Step 2 Select a running job and click **Delete**.

A message appears, `Selected job(s) will be deleted`.

Step 3 Click **OK**.

Viewing the Configuration Archive Job Details

From the Archive Management Jobs window, you can learn more about one job by viewing its details. You can view these details by clicking the Job ID on the Config Job window.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

The Archive Management Job Details window contains the following information:

Page/Folder	Description
Execution Summary	Displays summary of completed job: • Execution Summary—Information about the job status, start time and end time. • Device Summary—Information about the job completion status on the devices you have selected. For example, number of successful devices where the job is executed successfully. Click on Device Details folder and device status link and on the Device link to see the complete job execution details. • Execution Message (Pre-Execution and Post-Execution)—Information about any e-mails sent.
Device Details	Contains detailed job results for each device. Displays status folders that correspond to possible device status: • Successful Devices—Devices were successfully executed. • Failed Devices—Devices were not successfully executed. • Partially Failed Devices—Job partially failed to run on these devices. • Pending Devices—Job did not try to update devices, even though they were selected. • Not Attempted—Job did not attempt to run on these devices. Click on **Status** to see the job details. Details include a record of the entire CLI session between LMS and the device. When the configuration fetch takes unusually long, this error message appears, `Unable to get results of job execution for device. Please retry the job` This could happen because of slow device response, Network latency, etc.
Work Order	Contains the Summary of the job definition such as, • Detailed information, such as owner, schedule type, and Job Approval state. • Policies configured for the job, such as E-mail Notification and Job Based Password. • Devices on which the job runs. Also, gives details about the commands. For retried jobs, these job definitions are not updated. For such jobs the original job definitions are retained.

The buttons on the Job Details window are:

- Delete—You can delete jobs with the following Job Status:
  - Cancelled
  - Failed
  - Scheduled
  - Rejected
  - Successful
  - Waiting for Approval

You cannot delete a running job.

- Stop—You can stop the following running job types (See Using Configuration Archive Job Browser for details on the job types):
  - Put Config
  - Import Config
  - Write to Running Config
  - Write to Startup Config
  - Copy Running Config to Startup
  - Copy Startup Config to Running
  - Reload Device
  - Config Quick Deploy
  - Check Compliance and Deploy
  - Deploy Baseline template
  - Compliance check

CHAPTER 6

Using Baseline Templates to Check Configuration Compliance

This chapter contains the following:

What is a Baseline Template?

Baselining refers to identifying a set of standardized policy based commands that you would want to have on a set of devices. You can create a Baseline template containing a set of commands identified through the baselining process. This template contains placeholders for device-specific values to be substituted.

For example:

`set vtp domain` [*name*] **`password`** [*xxx*]

`set snmp community read-write` [*Read write community string*]

Where *name*, *xxx* and *Read write community string* are variables that are substituted with the values you provide.

You can compare the Baseline template with the configuration of devices in the archive. You can also generate a non-compliance configuration report and deploy this template onto the devices to make it compliant. You can deploy a Baseline template to a group of devices by just scheduling one job.

When you add a new device of the same type to the network, you can use the existing Baseline template, which consists of two parts, command and values. You can create configurations for any device of the same type in the network by specifying the values for the variables in the Baseline template.

Sample Input file for Baseline Template

You can use the following input file for creating Baseline template:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <ConfigTemplate Name="Banner1" DeviceFamily="268437899,268438038" Version="1">
    - <Commandlet Name="Commands" ControlStmt="false" Parent="none" Submode="false"
    Condition="false" Ordered="false">
        - <CommandInfo CheckType="1">
          <Command>banner motd "******************** WARNING ****************************
        <NL>This is a private system and only authorized individuals are allowed!<NL>All
        others will be prosecuted to the fullest extent of the law!
        <NL>**************************************************************************"****
        </Command>
      </CommandInfo>
      <ContextModeCommand />
      <PreCondition />
  </Commandlet>
  </ConfigTemplate>
```

Handling Multi-line Commands in Baseline

Multi-line commands should be separated with <NL> tag and should be in the same line within the template.

You can use the following command to run the compliance check. This is considered as a single line command:

Below is the command that the customer can use in the compliance check for this use case. Please note this is a single line command.

```
+ banner motd "************************ WARNING ************************************
<NL>This is a private system and only authorized individuals are allowed!<NL>All others
will be prosecuted to the fullest extent of the law!
<NL>**************************************************************************"
```

Features of Baseline Templates

The features of Baseline templates are:

- You can use this Baseline template to compare with other device configurations and generate a report that lists all the devices that are non-compliant with the Baseline template.
- You can easily deploy the Baseline template to the same category of devices in the network.
- You can schedule a compliance check job and deploy the Baseline template on the non-compliant devices. This can be performed as a single job or as a separate job.
- You can import or export a Baseline template. This template is stored in XML format.

The rules for specifying the Baseline templates are:

- All the commands that are disallowed should begin with a "-".
- All commands that are mandatory should begin with a "+".
- All comment entries should begin with a "#".
- Commands that do not begin with (- or +) are considered as comments and ignored.
- The command values can be a wildcard match.

  + ip address [*ip-address*] [*netmask*]

  + ip address [**#10\.76\.38\..*#**] [*netmask*]

  + ip address [**#10\.72\..*\..*#**] [*netmask*]

  To find a match for any octet in an IP address you must use **\..***.

  In the examples shown above, the command will apply for all the devices with the IP address starting with 10.76.38.* [netmask] and 10.72.*.* [netmask].

- The regular expressions must be enclosed with **#**.

  For example:

  snmp-server location [#.*#]

  This command will fail compliance check for snmp-server location loc1 loc2 loc3, because the check will be performed only for one word after snmp-server location.

  To overcome this, you have to define the command as:

  + [# **snmp-server location** .*#]

  Then the compliance check will be performed for all forms of snmp-server commands like snmp-server location loc1 loc2.....n,etc.

- Negation in Regular expressions :

  Example 1: When there are multiple entries in the configuration files.

  Let us say, the commands in the device configuration are:

  logging name1

  logging name2

  logging name3

  The command available in the template is:

  +logging [#!name1#]

  Based on the command in the template, the negation of name1 is done. This returns true as there are other logging commands present with other names. So the template is compliant.

Example 2: When there is only one entry in the device configuration file.

Let us say, the command in the device configuration is:

logging name1

The command available in the template is:

```
+logging [#!name1#]
```

Based on the command in the template, the negation of name1 is done. This returns False, as there is no other command in the device configuration file with logging statement except *logging name1*. So the template is non-compliant.

Example 3: When there are no logging commands in the device configuration files.

Let us say, the command in the device configuration is:

No logging commands

The command available in the template is:

```
+ logging [# !name1 #]
```

Based on the command in the template, the negation of name1 is done. This returns False, as there are no login commands. So the template is non-compliant.

- The Baseline template uses java.util.regex engine for regular expressions. For more information, see the regex API guide for Java 1.4.2 from Oracle:

  http://download.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html

- Submode commands are provided only if the commands are to be compared inside a submode.

  For example:

  `interface` [#*Ethernet*.*#]

  `+ no shutdown`

  The `no shutdown` command will apply to all Ethernet interfaces.

Defining Commandsets

The commandsets are a set of one or more CLI commands. You can define a commandset while creating a Baseline template in the Advanced mode.

The features of the commandsets are:

- If the commands in commandset are in a submode (ip/interface etc.) a submode command must be specified for such a commandset.
- Commandsets can have one or more child commandsets.
- Child commandsets inherit parent's sub-mode command.

You can define commandsets that have to be checked before running the actual commands.

The features of the prerequisite commandsets are:

- A commandset can have another commandset as its prerequisite.
- A prerequisite commandset is used only for comparison and is not deployed onto the device.
- A commandset is compared with the config only if its prerequisite condition is satisfied.

LMS evaluates the commandsets in different ways depending on whether you have defined the commandset as Parent or Prerequisite.

For example, assume that you have defined two commandsets, commandset1 and commandset2:

- Commandset defined as Prerequisite

  commandset1 as the Prerequisite of commandset2. When LMS evaluates the Baseline template, it evaluates commandset1 first, and commandset2 next.

  If commandset1 does not contain submode and is not present in a device, then commandset2 is not evaluated and the device is displayed in the excluded list in the compliance report.

  If commandset1 contains submode and is not present in applicable submodes, then commandset2 is not evaluated and the device is displayed in the excluded list in the compliance report.

- Commandset defined as Parent

  commandset1 as the Parent of commandset2. When LMS evaluates the Baseline template, it evaluates commandset1 first, and commandset2 next.

  If either of these commandsets is missing, the template is considered non-compliant.

Baseline Template Management Window

To access the Baseline Template Management Window go to **Configuration > Compliance > Compliance Templates > Templates.**

This window lists all the system-defined and user-defined Baseline templates. It also displays the following details of the Baseline template:

Column Name	Description
Name	Name of the Baseline template. The following template examples are displayed, by default: • CISF_DHCP_Snooping—Template for Catalyst Integrated Security Feature • TemplateExample1—Basic template with Regular expression • TemplateExample2—Advanced template with Submode and Parent, child options • TemplateExample3—Advanced template with prerequisite options • TemplateExample4—Advanced template with ordered set options • VRFCompliance—Template for VRF Compliance Click the template name to view the command sets. For more information, see Command Sets.
Device Type	Type of device for which the defined Baseline template can be used.
Description	Description of the Baseline template. If you have imported Baseline templates, the description given is *Imported*.
Created On	Displays the Baseline template creation date and time.

You can click on any column to sort the information by that column. If you double-click a heading, the order is reversed.

This window contains the following buttons:

Button	Description
Edit	Edit a Baseline template. This button is active only after you select a Baseline Template. See Editing a Baseline Template for further details
Export	Export a Baseline template file. This button is active only after you select a Baseline Template. See Exporting a Baseline Template for further details.
Delete	Delete a Baseline template. This button is active only after you select a Baseline Template. See Deleting a Baseline Template for further details.
Create	Create a Baseline template. See Creating a Baseline Template for further details.
Import	Import a Baseline template file. See Importing a Baseline Template for further details.

Command Sets

To view the template command sets:

Step 1 Go to **Configuration > Compliance > Compliance Templates > Templates.**

The Baseline Templates window appears, displaying the list of all the user-defined Baseline templates.

Step 2 Click the template name. For example, CISF_DHCP_Snooping.

The BaseLine Config Viewer window appears, displaying the command sets used in the template.

Table 6-1 provides information on the command sets used in the template examples.

Table 6-1 Command Sets

Template	Command Sets
CISF_DHCP_Snooping	Name: Commands SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none `+ ip dhcp snooping`
TemplateExample1	Name: Commands SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none `+ snmp-server community [#.*#] RW`

Table 6-1 Command Sets

Template	Command Sets
TemplateExample2	Name: Global SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset : none Parent: none Name: parent SubMode: Yes isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none policy-map V3PN-teleworker Name: child SubMode: Yes isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: parent class VOICE `+ priority 64`

TemplateExample3	Name: Global SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none
	Name: prereq SubMode: No isPrerequisite: Yes Ordered: No Prerequisite-Commandset: none Parent: none
	`+ class-map match-all GOLD`
	Name: parent SubMode: Yes isPrerequisite: No Ordered: No Prerequisite-Commandset: prereq Parent: none policy-map GSB_Policy
	Name: child SubMode: Yes isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: parent class GOLD
	`+ bandwidth percent 25`

TemplateExample4	Name: Global SubMode: No isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none
	Name: acceslist SubMode: No isPrerequisite: No Ordered: Yes Prerequisite-Commandset: none Parent: none
	`+ access-list 101 deny tcp 10.77.209.0 0.0.0.255 any`
	`+ access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23`
	`+ access-list 101 permit ip any any`

VRFCompliance	Name: Commands SubMode: Yes isPrerequisite: No Ordered: No Prerequisite-Commandset: none Parent: none interface [#.*#] `+ ip vrf forwarding [#red|green|blue#]`

Editing a Baseline Template

You can edit all Baseline template fields except for Template Name.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To edit the Baseline templates:

Step 1 Select **Configuration > Compliance > Compliance Templates > Templates**.

The Baseline Templates dialog box appears.

Step 2 Select a Baseline template.

Step 3 Click **Edit**.

The Select Creation Mode dialog box appears. The mode that you have selected while creating the Baseline template is retained. You cannot change this mode.

- You can provide a description in the Description text field.
- You can select or deselect devices in the Device Type Selector listbox.

Step 4 Click **Next.**

The Add Template Details dialog box appears.

Step 5 Select the commandset that you want to edit.

Step 6 Edit the required information.

See Creating an Advanced Baseline Template for more information on field descriptions for the fields that appear in the Add Template Details dialog box.

Step 7 Click **Finish**.

A message appears, `Template is modified. Do you wish to save the changes?`

Step 8 Click **OK**.

A notification appears, `Successfully updated the template` *BaselineTemplateName*.

Step 9 Click **OK** to save changes.

Exporting a Baseline Template

You can export a Baseline template. The exported file is in XML format.

The default path in the LMS Server to which the XML file is exported to is:

- *NMSROOT*\files\rme\dcma\baselinetemplates *(*On Windows*)*
- /var/adm/CSCOpx/files/rme/dcma/baselinetemplates (On Solaris and Soft Appliance)

Where, *NMSROOT* is the LMS installed directory.

You cannot change the default export path in the LMS Server. If you do so, an error message will be displayed.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To export a Baseline Template:

Step 1 Select **Configuration > Compliance > Compliance Templates > Templates**.

The Baseline Templates dialog box appears.

Step 2 Select one or more Baseline templates and click **Export**.

The Export a Baseline Template dialog box appears.

Step 3 Click **Browse**.

The Server Side File Browser dialog box appears.

Step 4 Select a folder.

Step 5 Click **OK** in the Server Side File Browser dialog box.

Step 6 Click **OK**.

A message appears, `CMA0086: Selected Template(s) are successfully exported.`

The naming convention followed for the baseline parameter file is *Template Name*.xml.

The file will be exported to the default location at the specified path in XML format.

Deleting a Baseline Template

To delete a baseline template:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Compliance > Compliance Templates > Templates**.

The Baseline Templates dialog box appears.

Step 2 Select one or more Baseline templates and click **Delete**.

A message appears, `The selected Template will be permanently deleted.`

You can delete only user-defined templates and not system-defined templates.

Step 3 Click **OK**.

A message appears, `Successfully deleted the template.`

Step 4 Click **OK**.

The selected Baseline Template is removed from the Baseline Templates window

Note You cannot delete Example Templates.

Creating a Baseline Template

You can create a Baseline Template by:

- Creating a Basic Baseline Template
- Creating an Advanced Baseline Template

There are few example templates that are available. You can use these templates as a base to create new templates.

- Creating a Basic Baseline Template - an Example
- Creating an Advanced Baseline Template— Example

Note View Permission Report (**Reports** > **System** > **Users** > **Permission**) to check if you have the required privileges to perform this task.

Creating a Basic Baseline Template

To create a Basic Baseline template:

Step 1 Select **Configuration** > **Compliance** > **Compliance Templates** > **Templates**.

The Baseline Templates window appears.

Step 2 Click **Create**.

The Select Creation Mode dialog box appears.

Step 3 In the Template Details section, select **Basic** as the mode.

Step 4 Enter the following information:

Field	Description
Name	Name of the Baseline template. You can enter up to 254 alphanumeric characters (including underscores). Do not enter special characters, including spaces and hyphens.

Field	Description
Description	Description for the Baseline template. You can enter up to 254 characters.
Device Type Selector	Device family to which you can apply this template. Click the check box to select the device family.

Step 5 Click **Next**.

The Add Template Details dialog box appears.

Step 6 Enter the following in the Baseline Template page.

Field	Description
Conditional Block	
Check for compliance only if the following condition is satisfied.	Check this option if you want to run a compliance check based on any condition.
Global	Select this option if you want to check the conditional commands in Global mode. This option is activated only if **Check for compliance only if the following condition is satisfied** is checked.
Submode	Select this option if you want to check the conditional commands in a specific submode. If you select this option, the textbox next to this option is activated. Enter the command for the required submode. For example: `interface` [*#Ethernet.*#*] This option is activated only if the **Check for compliance only if the following condition is satisfied** option is checked.

CLI Commands	Enter the conditional CLI commands in this text area.
	This option is activated only if **Check for compliance only if the following condition is satisfied** is checked.
	Enter the Conditional CLI commands.
	For example:
	`# Routers CLI Commands`
	`+ set snmp community read-write` [*read-write-community-name-string*]
	`- set snmp community read-only public`
	Explanation:
	• The first line is considered as a comment as it does not begin with either "+" or "-".
	• The second line is mandatory as it begins with "+".
	• The third line is disallowed as it begins with "-".
	In the above example, *read-write-community-name-string* is a command value. The command value should not contain spaces.

Compliance Block	
Global	Select this option if you want to check the compliance commands in global mode.

Field	Description
Use the SubMode of above condition	This option is activated only if the Conditional Block options, **Check for compliance only if the following condition is satisfied** and the Submode options are selected. The submode command entered in the submode textbox under the Conditional Block appears in the submode textbox of Compliance Block. So, the submode command of the Conditional Block is used by the Compliance Block. You cannot edit the submode commands in the Compliance Block. However, you can edit the submode commands in the Conditional Block, which in turn updates the submode commands in the Compliance Block.
Submode	Select this option if you want to check the compliance commands in a specific submode. If you select this option, the textbox next to this option is activated. Enter the command for the required submode. The compliance command will be checked for the submode that you enter.

CLI Commands	Enter the Compliance CLI commands. This is a mandatory field.
	For example, you can enter:
	`Routers CLI Commands`
	`# this is the Compliance Block`
	`+ set snmp community read-write` [*read-write-community-name-string*]
	`- set snmp community read-only public`
	Explanation:
	• The first line is considered as a comment as it does not begin with either "+" or "-".
	• The second line is also considered as a comment as it begins with a "#".
	• The third line is mandatory as it begins with "+".
	• The fourth line is disallowed as it begins with "-".
	In the above example, *read-write-community-name-string* is a command value. The command value should not contain spaces.

Order Sensitive	Select this option to make the system consider the order of the commands while performing a compliance check. In other words, the commands in the device config should appear in the same order as that of the CLI commands definition order in the Command Set.

- If you want to preview the changes to the template command details before the template is created, click **Preview**. The changed template details are displayed in a window.
- If you want to reset the changes click **Reset**.
- If you want to know about the options and the functionality of Basic flow click **Help**.

You can perform a Compliance check without using the Conditional Block.

A message appears, `Successfully created the template` *BaselineTemplateName*.

Where *BaselineTemplateName* is the Template Name as given by you.

Step 7 Click **OK**.

The Baseline Templates window appears with the newly created Baseline template.

Creating a Basic Baseline Template - an Example

You want to create a baseline template to check if all Ethernet interfaces that are up and running have "10.77.*.*" IP Address configured with the subnet mask 255.255.255.128.

To perform this task, you must create a template that checks for the following compliances:

- If there are interfaces that do not contain the `shutdown` command.

  and

- If all Ethernet interfaces are configured with IP address 10.77.*.* 255.255.255.128.

You can create a Basic Baseline Template by entering the condition check, as well as the compliance check.

To create a Basic Baseline Template for the above scenario:

Step 1 Select **Configuration** > **Compliance** > **Compliance Templates** > **Templates**.

The Baseline Templates window appears.

Step 2 Click **Create**.

The Select Creation Mode dialog box appears.

Step 3 In the Template Details section, select **Basic** as the mode.

Step 4 Enter the following information:

Field	Description
Name	Enter *NewBaseline* *NewBaseline* is the name of the new template.
Description	Enter the following description: This is a Basic Baseline template that checks if all Ethernet interface are up and running and have "10.77.*.*" IP address configured with the subnet mask 255.255.255.128
Device Type Selector	Check the Routers checkbox to select all routers.

Step 5 Click **Next**.

The Add Template Details dialog box appears.

Step 6 Select **Check for compliance only if the following condition is satisfied** so that you can enter the condition to be checked.

Step 7 Select **Submode**

The textbox next to Submode is activated.

Step 8 Enter the following command in the Submode textbox:

`interface` [*#Ethernet.*#*]

Step 9 Enter the following Conditional CLI commands in the Conditional Block CLI command text area:

`- shutdown`

This command indicates that `shutdown` should not be present in the Ethernet interfaces.

Step 10 Go to Compliance Block

The **Use the SubMode of above condition** option is selected automatically.

Step 11 Enter the following CLI commands in the Compliance Block CLI command text area:

```
+  ip address [#10.77.*.*#] 255.255.255.128
```

This command helps you to ascertain if the specified IP addresses are configured on the Ethernet interfaces.

Step 12 Click **Finish**

A message appears, `Successfully created the template` *NewBaseline*.

Where *NewBaseline* is the Template Name as entered by you.

Step 13 Click **OK**.

The Baseline Templates window appears with the newly created Baseline template.

Creating an Advanced Baseline Template

To create an Advanced Baseline template:

Step 1 Select **Configuration > Compliance > Compliance Templates > Templates**.

The Baseline Templates dialog box appears.

Step 2 Click **Create**.

The select Creation Mode dialog box appears.

Step 3 Select **Advanced** as the mode from the Template Details section.

Step 4 Enter the following information:

Field	Description
Name	Name of the Baseline template. You can enter up to 254 alphanumeric characters (including spaces). Do not enter any special characters, including underscores and hyphens.
Description	Description for the Baseline template. You can enter up to 254 characters.
Device Type Selector	Device family for which you can apply this template. Check the check box to select the device family.

Step 5 Click **Next**.

The Add Template Details dialog box appears.

Step 6 Enter the following information:

Field	Description
Commandset Options	
Name	Name of the commandset. You can enter only alphanumeric characters up to 254 characters. Do not enter any special characters. This includes spaces, underscores and hyphens.

Field	Description
Parent	Enter the parent name for the commandset, if required. This is case sensitive. You can also use this to logically group the commandsets. For example: To work on ATM permanent virtual connections (PVCs) commands, you must first get into the interface mode from the global mode and then run the PVC specific-commands. Commandset 1: ATM `interface` *[#atm.*#]* `+ ip address` *[ip-addr] [net-mask]* Commandset 2: PVC *[#pvc.*#]* `+ encapsulation aal5` *[encap-type]* `+ abr` *[output-pcr1] [output-mcr]* `+ ubr` *[output-pcr2]* `+ vbr-nrt` *[output-pcr3] [output-scr] [output-mbs]* `+ vbr-rt` *[peak-rate] [average-rate] [burst]* `+ protocol ip` *[proto-ip] [type]* `+ exit` Here, commandset 1 is the parent for commandset 2. LMS evaluates the Baseline template, commandset1 is evaluated first and commandset2 is evaluated next. If either of these commandsets is missing, the template is considered as non-compliant.
Prerequisite	Select the mandatory commandset name that you must enter before running the current commandset. In the example (See Mark as Prerequisite row), if you had marked commandset 1 as the Prerequisite, you can select *commandset 1: IntCheck* from the drop-down menu. Before running the commandset 2, the commandset 1 is run. That is, commandset1 is evaluated first and commandset2 is evaluated next. If there is no commandset1 or commandset1 failed, commandset2 is not evaluated and the devices will be moved to excluded state. The template will be considered as non-compliant.

Field	Description
Mark as Prerequisite	1. Select the checkbox to mark a particular commandset as a prerequisite. For example, Commandset 1: IntCheck **`interface`** *[intname]* **`+ ip address`** *[#10\.76\.38\..*#] [net-mask]* (To find a match for any octet in an IP address you must use `\..*`.) 2. Select the Mark as Prerequisite check box for the *Commandset 1: IntCheck*. For example, Commandset 2: IntDownload **`interface`** *[intname]* **`+ no cdp enable`** 3. Select the Prerequisite from the dropdown menu for the *Commandset 2: IntDownload*. If a commandset has a Prerequisite commandset, you cannot select the Mark as Prerequisite check box for that particular commandset. That is, in the above example, you cannot select the checkbox Mark as Prerequisite for *Commandset 2:IntDownload*.
CLI Commands	
Submode	Enter the command to get into interface mode from the global mode. For example: **`interface`** [*intname*] Here, **`interface`** is a command keyword and *intname* is command value. The command value should not contain spaces. You can also run the command for a set of interfaces. For example: **`interface`** [*#Ethernet.*#*] Here, the command will be executed on all the interfaces having Ethernet.

Field	Description
Ordered Set	Select this option to make the system consider the order of the commands while performing compliance check. In other words, the commands in the device config should appear in the same order as that of the CLI commands definition order in the Command Set. See, Behavior of Ordered Set for Access Lists for more details on the behavior of Ordered Set for Access Lists.

CLI Commands	Enter the CLI commands.
	For example:
	`# Routers CLI Commands`
	`+ set snmp community read-write` [*read-write-community-name-string*]
	`- set snmp community read-only public`
	Explanation:
	• The first line is considered as a comment as it begins with a "#".
	• The second line is mandatory as it begins with "+".
	• The third line is disallowed as it begins with "-".
	There should be a space between the commands and the "-" or "+". If there is no space, the commands are considered as comments and ignored.
	In the above example, *read-write-community-name-string* is a command value. The command value should not contain spaces.

- If you want to add a new commandset to the template click **Add**. The CLI Commands window is displayed with the default help comments. These help comments serve as guidelines to create commandsets.
- If you want to delete a Commandset from the Command set list, click **Delete**.
- If you want to preview the changes to the Commandset details before finishing up the creation of the template, click **Preview**. The changed Commandset details is displayed in a window.
- If you click **Save**, for the first time, the following message appears,
  `Do you wish to create a new template?.`
- If you click **Save**, for the second time, the following message appears,
  `Successfully updated the template` *BaselineTemplateName*.

Note If the Commandsets consist of Prerequisite commandset then these commandsets appear in red color in the Preview details.

- If you want to reset the changes made to a Commandset, click **Reset**

Step 7 Click **OK**.

A message appears,

`Successfully created the template` *BaselineTemplateName*.

Where *BaselineTemplateName* is the name of the Baseline Template.

Step 8 Click **OK**.

If you want to add one more commandset repeat this procedure from Step 4.

Step 9 Click **Finish**.

A message appears,

```
Do you wish to save the changes?.
```

Step 10 Click **OK**.

A message appears,

```
Successfully created the template.
```

Step 11 Click **OK**.

The Baseline Configs window appears with all the available Baseline templates.

Creating an Advanced Baseline Template— Example

This section consists of two examples:

- Example 1
- Example 2

Example 1

This is a procedure to create a Baseline template to disable CDP on an interface that belongs to a specific subnet.

Step 1 Select **Configuration > Compliance > Compliance Templates > Templates**.

The Baseline Templates dialog box appears.

Step 2 Click **Create**.

The Select Creation Mode dialog box appears.

Step 3 Select **Advanced** and click **Next**.

The Create a Baseline dialog box appears.

Step 4 Enter the following information:

Field	User data
Template Name	DisablingCDP You can enter up to 254 alphanumeric characters. Do not enter any special characters, except underscores.
Device Type	Routers
Description	Baseline Template for DisablingCDP
Commandset Option	
Name	PrerequisiteCheck. You can enter up to 254 alphanumeric characters. Do not enter any special characters including spaces, underscores and hyphens.

Field	User data
Parent	Global
Prerequisite	Do not select any value.
Mark as Prerequisite	Select the check box to mark the commandset as prerequisite.
CLI Commands	
Submode	interface [*intname*] Where, *intname* is a variable. The variables should not contain spaces.
Ordered Set	Select this so that the system orders commands while performing compliance check. See, Behavior of Ordered Set for Access Lists for more details on the behavior of Ordered Set for Access Lists.
CLI Commands	`+ ip address` *[#10\.76\.38\..*#] [netmask]* To find a match for any octet in an IP address you must use `\.[0-9]{1,3}`. This checks for subnet mask with IP address starting from 10.76.38.*.

Step 5 Click **Save**.

A message appears to say that the template will be created.

Step 6 Click **OK**.

A message appears to say that the template is created.

Step 7 Click **OK**.

To add another commandset to the same Baseline template, Disabling-CDP, enter the following information.

Field	User Data
Commandset Option	
Name	DisableCDP. You can enter up to 254 alphanumeric characters. Do not enter any special characters. This includes spaces, underscores and hyphens.
Parent	Global
Prerequisite	Select the PrerequisiteCheck from the dropdown menu.
Mark as Prerequisite	Do not select the checkbox.
CLI Commands	
Submode	interface [*intname*]
Ordered Set	Select this so that the system orders commands while performing compliance check.
CLI Commands	`+ no cdp enable` This will disable the CDP in all the interfaces even if any one interface contains the subnet mask starting with IP address 10.76.38.*.

Step 8 Click **Save**.

A message appears to say that the template is updated.

Step 9 Click **OK**.

Step 10 Click **Finish**.

A message appears to say that the template will be saved.

Step 11 Click **OK**.

A message appears to say that the template is updated.

Step 12 Click **OK**.

The Baseline Configs window appears with the details of Disabling-CDP Baseline template.

Example 2

This is a procedure to create an Advanced Baseline Template to check the presence of the command "ip address 10.77.209.8 255.255.255.224" in the Ethernet interfaces that have CDP disabled.

Step 1 Select **Configuration** > **Compliance** > **Compliance Templates** > **Templates**.

The Baseline Templates dialog box appears.

Step 2 Click **Create**.

The Select Creation Mode dialog box appears.

Step 3 Select **Advanced** and click **Next**.

The Create a Baseline dialog box appears.

Step 4 Enter the following information:

Field	User Data
Template Name	CheckIPTemplate You can enter up to 254 alphanumeric characters. Do not enter any special characters except underscores.
Device Type	Routers
Description	Baseline Template for Interface level check.
Commandset Option	
Name	PrerequisiteCheck. You can enter up to 254 alphanumeric characters. Do not enter any special characters including spaces, underscores and hyphens.
Parent	Do not enter anything.
Prerequisite	Do not select any value.
Mark as Prerequisite	Select the check box to mark the commandset as prerequisite.
CLI Commands	
Submode	interface [#Ethernet.*#]
Ordered Set	Do not select the checkbox.
CLI Commands	`+ no cdp enable`

Step 5 Click **Save**.

A message appears to say that the template will be created.

Step 6 Click **OK**.

A message appears to say that the template is created.

Step 7 Click **OK**.

To add another commandset to the same Baseline template, CheckIPTemplate, enter the following information.

Field	User data
Commandset Option	
Name	IPCheck. You can enter up to 254 alphanumeric characters. Do not enter any special characters including spaces, underscores and hyphens.
Parent	PrerequisiteCheck
Prerequisite	Select the PrerequisiteCheck from the dropdown menu.
Mark as Prerequisite	Do not select the checkbox.
CLI Commands	
Submode	Do not enter anything
Ordered Set	Do not select the checkbox.
CLI Commands	`+ ipaddress` *10.77.209.8 255.255.255.224* The above command will be deployed on the Ethernet interfaces that have CDP disabled.

Step 8 Click **Save**.

A message appears to say that the template is updated.

Step 9 Click **OK**.

Step 10 Click **Finish**.

A message appears to say that the template will be saved.

Step 11 Click **OK**.

A message appears to say that the template is updated.

Step 12 Click **OK**.

The Baseline Configs window appears with the details of CheckIPTemplate Baseline template.

Behavior of Ordered Set for Access Lists

1. Create a baseline template with few commands and ordered set option checked.
2. Compare the configurations in the device with the baseline template, to check for Compliance

   The commands available in the device is compared in the same order as available in the Baseline template.

3. If the commands found in the device are not compliant with the Baseline template, the same configlet commands available in the device are negated first and then the commands available in the Baseline template are deployed on the device.

This is the recommended behavior for Access lists. This behavior is also supported by the submodes.

Importing a Baseline Template

You can import a template as Baseline template. The imported file must be in XML format.

The default path in the LMS Server from which the XML file is imported is

- *NMSROOT*\files\rme\dcma\baselinetemplates *(*On Windows*)*
- /var/adm/CSCOpx/files/rme/dcma/baselinetemplates (On Solaris and Soft Appliance)

Where, *NMSROOT* is the LMS installed directory.

You cannot change the default import path in the LMS Server. If you do so, an error message will be displayed

To import a Baseline Template:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Compliance > Compliance Templates > Templates**.

The Baseline Templates dialog box appears.

Step 2 Select a Baseline template and click **Import**.

The Import a Baseline Template dialog box appears.

Click **Browse**.

The Server Side File Browser dialog box appears.

Step 3 Select the XML file.

Step 4 Click **OK** in the Server Side File Browser dialog box.

Step 5 Click **OK**.

A message appears, `Template successfully imported`.

Step 6 Click **OK**.

The imported file appears in the Baseline Templates window with the description, Imported baseline.

Running Compliance Check

To run a compliance check:

Step 1 Select **Configuration > Compliance > Compliance Templates > Compliance Check**.

The Baseline Templates dialog box appears.

Step 2 Select the template and click **Compliance Check**.

The Select Devices dialog box appears.

Step 3 Select either:

- Device Selector, if you want to schedule a job for a static set of devices. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Or

- Group Selector, if you want to schedule a job for a dynamic group of devices.

  The job is scheduled only for the devices that are present in the selected group at the time when the job is run. The customizable group selector for jobs evaluate static groups also as dynamic during run time.

Step 4 Click **Next**.

The Schedule dialog box appears.

Step 5 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Baseline template compliance job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the specified day of the week and at the specified time. • Monthly—Runs monthly on the specified day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not been completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) at which to schedule. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Attachment	Check this option if you want the job notification mail to consist of attachments in either CSV or PDF format. Select either: • CSV if you want the attachment in CSV format. Or • PDF if you want the attachment in PDF format. This is the default format. The CSV and PDF radio options will be enabled only if the Attachment checkbox is checked. If the Attachment option is disabled, go to **Admin > System > System Preferences** to change the settings. For more information on configuring attachment settings as well as the maximum size of attachments allowed in notification mails, see Administration Online Help.
Job Options	
Check compliance and deploy	Enable this to check the compliance of the archived file with that of the Baseline template and deploy the commands if it is non-compliant. This option is not supported for Group selector.
Copy Running Config to Startup	This option is active only if you select the Check compliance and deploy option. Select to make the job write the Running configuration to the Startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Job Password	• If you have enabled the Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either: – Enter the device login user name and password and device Enable password Or – Disable the Job Password option in the Job Schedule and Options dialog box.

Step 6 Click **Next**.

The Job Work Order window appears with the job details that you have selected.

Step 7 Click **Finish**.

A message appears, `Job` *JobID* `is created successfully`.

Where *JobID* is a unique Job number.

Step 8 Click **OK**.

You can check the status of your scheduled job by selecting **Configuration** > **Job Browsers** > **Configuration Archive**.

Note View Permission Report (**Reports** > **System** > **Users** > **Permission**) to check if you have the required privileges to perform this compliance check task.

The compliance check job requires approval if you have enabled Job Approval during the compliance check job scheduling.

For further details on the baseline template, see Understanding the Baseline Compliance Report.

Understanding the Baseline Compliance Report

The Baseline Compliance Report contains the following information:

Field Name	Description
Summary	
Template Name	Name of the Baseline template entered at the time of creating the Baseline template.
Number of Non-Compliant devices	Number of devices that are non-compliant.
Number of Compliant devices	Number of devices that are compliant.
Number of Excluded devices:	List of devices in which the job did not run. The jobs may have failed either because: • The device configuration was not archived. Or • The device was not reachable. Further details of the failed job are given in the **Configuration** > **Job Browsers** > **Configuration Archive** (See Using Configuration Archive Job Browser).
Compliant Devices	
Device Name	Device Display Name as entered in Device and Credential Repository.
Latest Version	Version of configuration file against which the compliance was checked. Click on the version to display Config Viewer (see Understanding the Config Viewer Window). This shows the contents of the corresponding configuration file against which the compliance was checked.
Created On	Date and time at which the configuration file was created.

Field Name	Description
Non-Compliant Devices	
Device Name	Device Display Name as entered in Device and Credential Repository.
Latest Version	Version of configuration file against which the compliance was checked. Click on the version to display Config Viewer (see Understanding the Config Viewer Window). This shows the contents of the corresponding configuration file against which the compliance was checked.
Created On	Date and time at which the configuration file was created.
Commands to Deploy	List the commands where the device configuration is non-compliant.
Excluded Devices	
Device Name	Device Display Name as entered in Device and Credential Repository.
Reason for Exclusion	Displays the cause for exclusion.

In addition, this report contains two buttons:

Button	Description
Export to File (Icon)	Exports this report in either PDF or CSV format.
Print (Icon)	Generates a format that can be printed.

Deploying a Baseline Template

When you add a new device of the same type to the network, you can use the existing Baseline template. This template consists of two parts, command and values.

You can create configurations for any device of the same type in the network by specifying the values for the variables in the Baseline template.

You can deploy Baseline template on the devices in two ways:

- User Interface (See Deploying a Baseline Template Using User Interface for the procedure.)
- File System (See Deploying a Baseline Template Using File System for the procedure.)

View Permission Report (**Reports** > **System** > **Users** > **Permission**) to check if you have the required privileges to perform this task.

The deployment job requires approval if you have enabled Job Approval during the deployment job scheduling.

Deploying a Baseline Template Using User Interface

To deploy a Baseline template using User Interface:

Step 1 Select **Configuration > Compliance > Compliance Templates > Direct Deploy**.

The Baseline Templates dialog box appears.

Step 2 Select a Baseline template and click **Deploy**.

The Deploy Input Options dialog box appears.

Step 3 Select **Enter Data From User Interface** and click **Next**.

The Select Devices dialog box appears.

The device list contains only devices of the type devices selected while creating the Baseline Template.

For example, if you have selected Device Type as Router, only routers are listed.

Step 4 Select devices under the following tabs:

- In the All tab,

  Devices are grouped under All Applicable Devices and All Applicable Device Groups. All Applicable Device Groups categorizes devices under Routers, Switches, and so on.
- In the Search Results tab,

  The results of simple search and advanced search are listed here.
- In the Selection tab,

  All the devices that are selected are listed and you can deselect the devices.

Step 5 Click **Next**.

The Commands Generation dialog box appears.

Step 6 Perform the following tasks:

Field Name	Description and Action
Device list	This pane lists the selected devices that you have selected in the Select Devices dialog box. Select the device for which you want to deploy the Baseline template.
Edit	Select a device from the device drop down list and click **Edit** to edit information for the device.
Save	Click **Save** to save the changes made for the selected device. You can change the details for multiple devices in one go, by using the Save button.
Device	The selected device in the Device List pane is displayed in this text box.
Commandsets	The pane contains all the commandsets that are defined in the Baseline template. Select a commandset. While creating the Baseline template, if you have defined the multiple occurrences as the commandset feature, after selecting that particular commandset, the *Add Instance* button is activated.

Field Name	Description and Action
Add Instance	This button is active only if you have selected a commandset with multiple occurrences. The occurrences of a commandset are defined while creating the Baseline template. When you click on the Add Instance button, one more instance of multiple commandset is added in the Commandsets pane. Enter the command value for that commandset in the Device Data pane.
Delete Instance	Use the Delete Instance button to delete the instance after selecting the instance from the Commansets pane. You can select one or more instances and click on the Delete Instance button to delete the instances. You can delete the selected instances. The exception being that at least one instance of the commandset is available.
Templates	The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.
Device Data	The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: **`Interface`** [*#Ethernet[.*]#*] **`+ no shutdown`** Then, *#Ethernet[.*]#* is the command value. The Device Data field names appear as: `#Ethernet.*`[*0*] If the commandset is a prerequisite commandset, you do not need to specify parameter values for the Device data field as they are not deployed.

Step 7 Click **Next**.

The Job Schedule dialog box appears.

Step 8 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Baseline template deploy job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the specified day of the week and at the specified time. • Monthly—Runs monthly on the specified day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule the job. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Job Options	
Approver Comments	Enter comments for the job approver. This field appears only if you have enabled job approval for Configuration Archive.
Maker E-Mail	Enter the e-mail-ID of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Configuration Archive.

Field	Description
Copy Running Config to Startup	Select to cause the job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) either: – Enter the device login user name and password and device Enable password Or – Disable the Job Password option in the Job Schedule and Options dialog box.

Step 9 Click **Next**.

The Work Order dialog box appears with job details that you have entered.

Step 10 Click **Finish**.

A message appears, `Job` *JobID* `is created successfully`.

Where *JobID* is a unique Job number.

Step 11 Click **OK**.

You can check the status of your scheduled job using **Configuration > Job Browsers > Configuration Archive**. The Job Type for this deploy job is Deploy Baseline template result.

Deploying a Baseline Template Using File System

You can deploy a Baseline template using the Baseline Parameter file.

The parameter file specifies the variable values for template deployment. To generate the parameter file:

Step 1 Select **Configuration > Compliance > Compliance Templates > Templates**.

Step 2 Click the hyperlink of the required template. The Baseline Config Viewer popup appears.

Step 3 Click Generate Param File. A popup appears.

Step 4 Click Browse to specify the folder with the parameter file.

See Exporting a Baseline Template for further information.

To deploy a Baseline template using File System:

Step 1 Select **Configuration > Compliance > Compliance Templates > Direct Deploy**.

The Baseline Templates dialog box appears.

Step 2 Select a Baseline template and click **Deploy**.

The Deploy Input Options dialog box appears.

Step 3 Select **Enter Data From File System** and click **Next**.

The Select Input File dialog box appears.

Step 4 Enter the folder name and the file name with the file format extension XML.

or

a. Click **Browse**.

The Server Side File Browser dialog box appears.

b. Select the XML file.

c. Click **OK**.

The Select Input File dialog box appears with the selected Baseline Parameter file.

Step 5 Click **Next**.

The Job Schedule dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Baseline template deploy job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the specified day of the week and at the specified time. • Monthly—Runs monthly on the specified day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule the job. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.

Field	Description
Job Options	
Approver Comments	Enter comments for the job approver. This field appears only if you have enabled job approval for Configuration Archive.
Maker E-Mail	Enter the e-mail-ID of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Configuration Archive.
Copy Running Config to Startup	Select to make the job write the Running configuration to the Startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) either – Enter the device login user name and password and device Enable password Or – Disable the Job Password option in the Job Schedule and Options dialog box.

Step 7 Click **Next**.

The Work Order dialog box appears with job details that you have entered.

Step 8 Click **Finish**.

A message appears, `Job` *JobID* `is created successfully`.

Where *JobID* is a unique Job number.

If you have specified incorrect filename/XML file format or if the hostname field is not updated, an error message appears, `Specified file could not be read. Please specify a valid file name`.

See Exporting a Baseline Template for further information.

Check the XML file format or update the hostname field and restart this procedure from Step 2.

Step 9 Click **OK**.

You can check the status of your scheduled job using **Configuration > Job Browsers > Configuration Archive**. The Job Type for this deploy job is Deploy Baseline template result.

Using Compliance and Deploy Jobs Window

You can check the status of the Baseline jobs using **Configuration > Compliance > Compliance Templates > Jobs.**

This section contains:

- Deploying the Commands
- Deleting the Compliance Jobs

This window contains the following information:

Field Name	Description
Job ID	Unique number assigned to the job when it is created. For periodic jobs such as Daily, Weekly, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001.
Description	Job description entered during job definition.
Compliant/Deployed Devices	Displays the number of devices that are compliant out of the total number of devices that were selected while creating the compliance job. Click on the link to view the Baseline Compliance Report (see Understanding the Baseline Compliance Report).
Status	Status of the job. The states can be Successful, Failed, and Running. The jobs may have failed either because: • The device configuration is not archived. Or • The device is not reachable. Further details of the failed job are given in the **Configuration > Job Browsers > Configuration Archive**. You can also check the status of the Baseline job at **Configuration > Job Browsers > Configuration Archive**.

The Baseline Jobs window contains the following buttons:

Buttons	Description
Deploy	You can schedule a job to deploy the standard configuration on all non-compliant devices. This button is active only after selecting a Job. See Deploying the Commands.
Retry	You can reschedule a failed job using this button. This button is active only on selecting a Failed job. Reschedule the deployment job by providing the required information.

Buttons	Description
Delete	You can delete the compliance jobs. This button is active only after selecting a Compliance Jobs. See Deleting the Compliance Jobs
Refresh (Icon)	Click on this icon to refresh the Compliance Jobs Window.

For usecases and examples on Baseline Templates, refer to the Baseline Template Whitepaper

Deploying the Commands

You can deploy the commands on the devices that are non-complaint.

Before you use this Deploy button, you must run the Compliance Report,

- If there are any non-complaint device, you must select the relevant compliance job and deploy the baseline template.
- If there are no non-complaint device and if you click on the Deploy button, a message appears,

```
Could not deploy selected Job.
Reason: No Non-Compliant devices present in the report.
```

Click on the Job ID to view the Baseline Compliance Report. See Understanding the Baseline Compliance Report for further details.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To deploy the commands:

Step 1 Select **Configuration > Compliance > Compliance Templates > Jobs**.

The Baseline Jobs dialog box appears.

Step 2 Select a Compliance Job.

Step 3 Click **Deploy**.

The Substitute Parameters for Devices dialog box appears.

Step 4 Perform the following:

Field Name	Description and Action
Device list	The list contains all the devices which are non-complaint. Select a device.
Device	The selected device in the Device List pane appears in this text box.

Field Name	Description and Action
Commandsets	The pane contains all the commandsets that are defined in the Baseline template. In the Baseline template, if you have defined the multiple occurrences as the commandset feature then based on the compliance check, the commandset will appear more than once. Select a commandset.
Templates	The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.
Device Data	The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: + **`ip address`** [*#10\.76\.38\..*#*] [*netmask*] Then, *#10\.76\.38\..*#* and *netmask* are the command values. The Device Data field names appear as: *#10\.76\.38\..*#*[1000] *netmask*[1000]

If you have more than one device to deploy then you have to repeat Step 4 for all the devices.

Step 5 Click **Next**.

The Job Schedule dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the deploy configuration job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time.
Date	You can select the date and time (hours and minutes) to schedule. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Attachment	Check this option if you want the job notification mail to consist of attachments in either CSV or PDF format. Either select: • CSV if you want the attachment in CSV format. Or • PDF if you want the attachment in PDF format. This is the default format. The CSV and PDF radio options will be enabled only if the Attachment checkbox is checked. If the Attachment option is disabled, go to **Admin > System > System Preferences** to change the settings. For more information on configuring attachment settings as well as the maximum size of attachments allowed in notification mails, see Administration Online Help.
Job Options	
Approver Comments	Enter comments for the job approver. This field appears only if you have enabled job approval for Configuration Archive.
Maker E-Mail	Enter the e-mail-ID of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Configuration Archive.
Copy Running Config to Startup	Select to make the job to write the Running configuration to the Startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either: – Enter the device login user name and password and device Enable password Or – disable the Job Password option in the Job Schedule and Options dialog box.

Step 7 Click **Next**.

The Work Order dialog box appears with job details that you have entered.

Step 8 Click **Finish**.

A message appears, `Job ID is created successfully`.

Where *ID* is a unique Job number.

Step 9 Click **OK**.

You can check the status of your scheduled job using **Configuration > Job Browsers > Configuration Archive**. The Job Type for this deploy job is Deploy Baseline comparison result.

Deleting the Compliance Jobs

You can delete the job that have been completed or stopped. You cannot delete a running job.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To delete Compliance jobs:

Step 1 Select **Configuration > Compliance > Compliance Templates > Jobs**.

The Compliance Jobs dialog box appears.

Step 2 Select a job and click **Delete**.

A message appears, `The selected job will be deleted`.

Step 3 Click **OK**.

The selected Compliance job is removed from the Compliance Jobs window.

You can also delete the compliance jobs from **Configuration > Job Browsers > Configuration Archive** window (see Using Configuration Archive Job Browser)

CHAPTER 7

Editing and Deploying Configurations Using Config Editor

The Config Editor provides easy access to configuration files. Config Editor allows a network administrator with the appropriate security privileges to edit a configuration file that exists in the configuration archive.

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 Inventory. It automatically tracks changes to configuration files and updates the database if a change is made.

You can open the configuration file, change it, and download it to the device.

- To start Config Editor from the LMS desktop, select **Configuration > Tools > Config Editor**.

  The Config Editor window appears.
- To set user preferences in Config Editor, select **Configuration > Tools > Config Editor > Edit Mode Preference**.

  The User Preferences window appears.

This section contains:

Config Editor Tasks

Config Editor users can:

- Open a configuration file version of a device for editing.
- Open configuration file version based on search criteria.
- Open an external configuration file.
- Save modified configuration file in private work area on the server and open the saved file when required.
- Save a configuration file in a public location.
- Send configuration file to syntax checker utility.
- Deploy configuration files to the device.
- Send configuration download jobs for approval.
- View all download jobs and perform job management operations.
- List out all the modified files, allow the user to select and download or close the configuration.
- Compare configurations that they are editing with the original configuration file version and other configuration versions of the selected device.
- Open a baseline configuration stored in config archive.

Benefits of Configuration Editor

Config Editor allows you to edit and download configuration files to devices using a GUI instead of the command line interface (CLI). Use Config Editor to edit individual device configurations within LMS and then download them again to the device.

A copy of the updated configuration will automatically be stored in the Configuration Archive. See Figure 7-1.

Figure 7-1 Config Editor Functional Flow

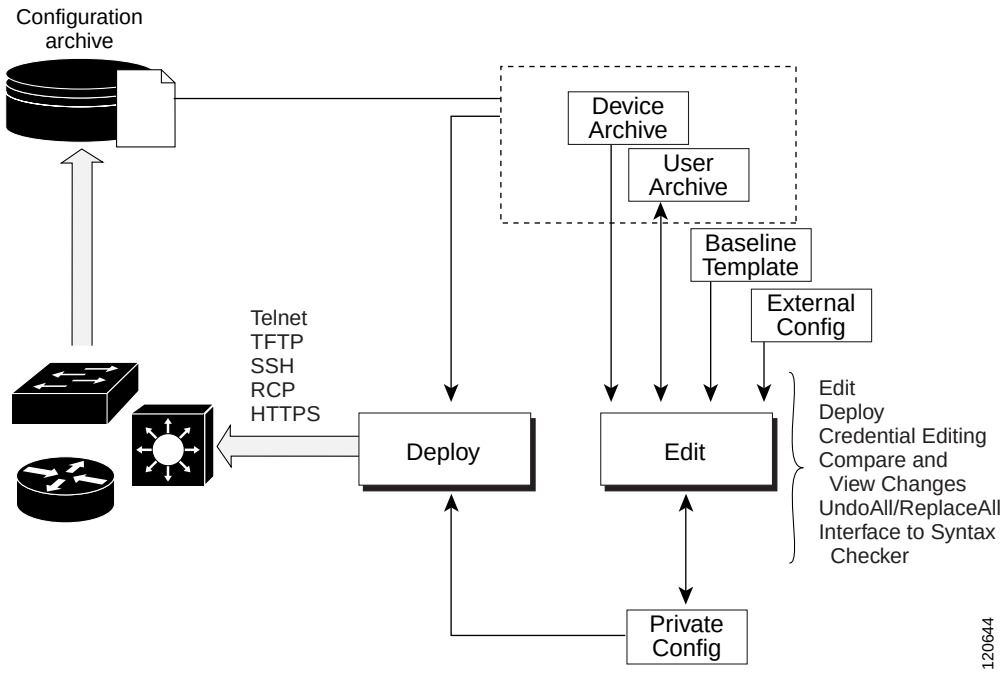


Table 7-1 shows the tasks you can accomplish with the Config Editor option.

Table 7-1 Config Editor Tasks

Task	Description	Action
Open a configuration file.	Open a configuration file for editing. You can open a configuration file in four ways: • Device and Version • Pattern Search • Baseline • External Location	Select **Configuration > Tools > Config Editor > Config Editor**.
Edit configuration files from the archives.	Edit a configuration file from the archive.	Select **Configuration > Tools > Config Editor > Config Editor > Device and Version > Edit.**

Table 7-1 Config Editor Tasks (continued)

Task	Description	Action
Edit a configuration file by pattern	Edit a configuration file by searching for a pattern. A pattern can be any text string.	Select **Configuration > Tools > Config Editor > Config Editor > Pattern Search > Finish.**
Edit a configuration file by baseline template	Create a baseline configuration from the baseline template maintained in configuration archive.	Select **Configuration > Tools > Config Editor > Config Editor > Baseline > Finish**.
Edit a configuration file by external location	Associate a device with the selected configuration file from an external location in the server.	Select **Configuration > Tools > Config Editor > Config Editor > External Location> Edit.**
Print configuration files.	Print a configuration file.	1. Select **Configuration > Tools > Config Editor > Config Editor**. 2. Select the configuration file and click **Edit**. 3. Select the Print icon at the top right corner.
Remove configuration file from the private area	Remove a configuration file from the private work area on the server.	1. Select **Configuration > Tools > Config Editor > Private Configs**. 2. Select the configuration file and click **Delete**.
Remove a configuration from the public work area	Remove a configuration file from the public work area on the server.	1. Select **Configuration > Tools > Config Editor > Public Configs.** 2. Select the configuration file and click **Delete**.
Save a configuration file in the public work area.	Save an edited configuration file in the public work area on the server and retrieve the saved file when required.	1. Select **Configuration > Tools > Config Editor > Public Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Save**.
Save a configuration file in the private work area.	Save an edited configuration file in the private work area on the server and retrieve the saved file when required.	1. Select **Configuration > Tools > Config Editor > Private Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Save**.
Undo editing or typing changes	Undo editing or typing changes when editing a file. You can undo editing changes of files in private or public work areas.	To undo editing changes of a file in the private work area: 1. Select **Configuration > Tools > Config Editor > Private Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Undo All**. To undo editing changes of a file in the public work area: 1. Select **Configuration > Tools > Config Editor > Public Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Undo All**.

Table 7-1 Config Editor Tasks (continued)

Task	Description	Action
Find and replace text	Find and replace all occurrences of the text when editing a configuration file in the Raw mode or find the text in a particular configlet in the Processed mode	To find and replace text of a file in the private work area: 1. Select **Configuration** > **Tools** > **Config Editor** > **Private Configs** 2. Select the configuration file and click **Edit**. 3. Click **Replace All**. To find and replace text of a file in the public work area: 1. Select **Configuration** > **Tools** > **Config Editor** > **Public Configs**. 2. Select the configuration file and click **Edit**. 3. Click **Replace All**.
Export Configuration File Changes	Exporting Changes of a Configuration File to a PDF file.	1. Select **Configuration** > **Tools** > **Config Editor** > **Config Editor**. 2. Select the configuration file and click **Edit.** 3. Select the **Export icon** at the top right corner.
Close Configuration File	Close a configuration file.	To close a configuration file in the private work area: 1. Select **Configuration** > **Tools** > **Config Editor** > **Private Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Close**. To close a configuration file in the public work area: 1. Select **Configuration** > **Tools** > **Config Editor** > **Public Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Close**.
Configure Job Policies.	Configure a default policy for job properties that applies to all future jobs. You can also specify whether the property can be modified when the job is created.	Select **Admin** > **Network** > **Configuration Job Settings** > **Config Job Policies**.

Table 7-1 Config Editor Tasks (continued)

Task	Description	Action
Set up the default editing mode.	Set up or change your default editing preferences. Config Editor remembers your preferred mode even across different invocations of the application. You can also change the mode when you open a configuration file using the Device and Version option. However, Config Editor does not remember this change across different invocations of the application. Only the changes made using the Admin function are remembered.	Select **Configuration > Tools > Config Editor > Edit Mode Preference**.
View changes	View the changes made to the opened configuration file. LMS compares the edited file with the original version.	To view changes made to a configuration file in the private work area: 1. Select Configuration > Configuration > Config Editor > Private Configs. 2. Select the configuration file and click **Edit.** 3. Click **Tools**. 4. Select **View Changes**. To view changes made to a configuration file in the public work area: 1. Select **Configuration > Tools > Config Editor > Public Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Tools**. 4. Select **View Changes**.

Table 7-1 Config Editor Tasks (continued)

Task	Description	Action
Compare versions of the configuration files.	Compare the edited files with any version in the Configuration Archive.	To compare versions of configuration files in the private work area: 1. Select **Configuration** > **Tools** > **Config Editor** > **Private Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Tools**. 4. Select **Compare Config**. To compare versions of configuration files in the public work area: 1. Select **Configuration** > **Tools** > **Config Editor** > **Public Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Tools**. 4. Select **Compare Config**.
View list of modified files.	View a list of files edited by all users in private or public work areas.	• To view a list of modified configuration files in private work area, select **Configuration** > **Tools** > **Config Editor** > **Private Configs**. • To view a list of modified configuration files in public work area, select **Configuration** > **Tools** > **Config Editor** > **Public Configs**.
Browse and edit Config Editor jobs.	Browse the Config Editor jobs that are registered on the system and edit them as necessary.	Select **Configuration** > **Job Browsers** > **Config Editor** > **Edit**.
View job details.	View detailed information about a registered Config Editor job and perform job management operations. You can also edit a job from its detailed view.	Select **Configuration** > **Job Browsers** > **Config Editor**.
Deploy a config	Define a deploy job. Defines jobs to deploy configuration files to the device.	Select **Configuration** > **Job Browsers** > **Config Editor** > **Create**.
Copy a job	Copy a job	Select **Configuration** > **Job Browsers** > **Config Editor** > **Copy**.
Delete a job	Delete a job	Select **Configuration** > **Job Browsers** > **Config Editor** > **Delete**.
Stop a job	Stop a job	Select **Configuration** > **Job Browsers** > **Config Editor** > **Stop**.

Table 7-1 Config Editor Tasks (continued)

Task	Description	Action
Check the configuration file syntax.	Check the syntax of the configuration file with an external syntax checker that is registered in CMIC Link registration.	To check the configuration syntax of a file in the private work area: 1. Select **Configuration** > **Tools** > **Config Editor** > **Private Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Tools** 4. Click **External Syntax Checker**. To check the configuration syntax of a file in the public work area: 1. Select **Configuration** > **Tools** > **Config Editor** > **Public Configs**. 2. Select the configuration file and click **Edit.** 3. Click **Tools** 4. Click **External Syntax Checker**.
Update DCR after deploy	Updates DCR after successfully deploying credential commands. This is applicable only for Telnet/SSH based download.	User configurable. An option is provided in the job creation flow.

Setting Up Preferences

You can use this feature to set up your editing preferences. Config Editor remembers your preferred mode, even across different invocations of the application.

You can change the mode using the Device and Version, Pattern Search, Baseline or External Configuration option but the changes do not affect the default settings.

To set up preferences:

Step 1 Select **Configuration** > **Tools** > **Config Editor** > **Edit Mode Preference**.

The User Preferences dialog box appears.

Step 2 Set the default edit mode:

- Select **Processed** to display the file in the Processed mode.

  The configuration file appears at the configlet level (a set of related configuration commands). The default edit mode is Processed.

- Select **Raw** to display the file in the Raw mode.

  The entire file appears as shown in the device.

Step 3 Click **Apply** to apply the specified preferences.

Overview: Editing a Configuration File

The Editor is a core component in Config Editor. It acts as the interface to open a configuration file, make a local copy, save the changed configuration and commit the changes back to the original location.

You can edit a file by:

- Selecting the device and the version of the configuration file
- Searching for a pattern
- Selecting a baseline configuration file
- Selecting a configuration file stored in an external location

You can edit a previously opened file, that is, a file from your private area or public work area.

You can edit the files in either the Raw or Processed mode.

- Raw mode—The entire file is displayed. After you open a file in a specific mode, you can view it only in that mode.
- Processed mode—Only the file commands are displayed at the configlet (set of related configuration commands) level.

Working With the Configuration Editor

You can use the editor to:

- Edit and save changes to the configuration file in public or private work area.
- Undo editing or typing changes
- Replace a string in opened configuration files
- Compare configuration files with the same device configuration
- View changes made in the configuration file
- Run Syntax Checker

This section contains:

- Processed Mode
- Raw Mode
- Editing Configuration Files by Handling Interactive Commands in Config Editor Jobs
- Modifying Credentials

The Editor window opens in Raw or Processed mode, based on your preference.

To launch the Editor:

Step 1 Select **Configuration > Tools > Config Editor > Config Editor**.

Step 2 Open a configuration file using any of the following methods:

- Using the selection criteria. See Overview: Opening a Configuration File
- Using Private Configs
- Using Public Configs

Using Private Configs

a. Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

   The List of Private Configs window appears.

   LMS converts the character ":" in the IPv6 address to "%03A". The Archive Name field in the List of Private Configs window might not display the actual IPv6 address.

b. Select the configuration and click **Edit.**

Using Public Configs

a. Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in public work area.

   The User Archived Configs window appears.

   LMS converts the character ":" in the IPv6 address to "%03A". The Name field in the User Archived Configs window might not display the actual IPv6 address.

b. Select the configuration and click **Edit.**

Step 3 Edit the credential commands in the Raw or Processed mode. See Processed Mode and Raw Mode.

Step 4 Select any of the following:

- **Save** to save changes to the configuration file. See Saving a Configuration File.
- **Save As** to save changes to the configuration file in a specified location.
- **Undo All** to undo editing or typing changes. See Undoing All.
- **Replace All** to replace a string in the opened configuration files. See Replacing All.
- **Deploy** to deploy a configuration file to a device.
- **Tools...** to launch the Config Editor tools. See Selecting Configuration Tools.
- **Close** to close the Config Editor window. See Closing a Configuration File.

Processed Mode

The configuration file appears at the configlet level (a set of related configuration commands). The default is Processed.

In the Processed mode, Editor window is divided into two panes.

- The left pane displays the configuration tree according to the grouping of configlets.
- The right pane displays the commands of configlets in two sections:
  - The lower section, called the credential area contains all the credential commands with the credentials masked. Click on the encrypted link to modify credentials.
  - The upper section, called the non-credential area contains only non-credential commands. The non-credential commands are editable.

Raw Mode

The entire file appears as shown in the device. After you open a file in a specific mode, you can view it only in that mode.

In Raw mode there are two sections for the entire configuration.

- The upper section, called the non-credential area contains only non-credential commands. The non-credential commands are editable.
- The lower section contains all the credential commands with the credentials masked. The credential commands can be edited.

Note Do not delete or edit the placeholder that describes the credential position. If you do so, the file generates errors.

Editing Configuration Files by Handling Interactive Commands in Config Editor Jobs

An interactive command is the input you will have to enter, after a command runs.

For example, in the case of Catalyst 5000 series devices, a command would be:

```
set vtp v2 enable
```

This command enables version 2 of VTP on the device. This command is an interactive command and requires user intervention after running the command.

You can download this command through ConfigEditor using:

```
#INTERACTIVE
set vtp v2 enable<R>y
#ENDS_INTERACTIVE
```

Such commands can be included in config jobs run using a Config Editor. You can handle interactive commands by editing configuration files.

To edit configuration files using interactive commands:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Click **Edit.**

The Editor window appears.

Step 3 Enter an interactive command in the configuration file, in the upper section that contains only non-credential commands using the following syntax:

```
#INTERACTIVE
command1<R>response1<R>response2
command2<R>response1<R>response2<R>response3
command3<R>response1
command4<R>response1<R>response2
#ENDS_INTERACTIVE
```

<R> tag is case-sensitive and this must be entered in uppercase only.

Step 4 Enter modification comments in the Change Description field.

Modifying Credentials

You can use this feature to modify or delete the credentials of a configuration file.To do this:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Click **Edit.**

The Editor window appears.

Step 3 Click the masked credential link in the With Credentials pane. (The masked credential appears as multiple *s.)

The Modify Credentials dialog box appears.

Step 4 Enter the information required to modify credentials.

Field	Description
Modify	Modifies credentials of the selected configlets.
Delete	Deletes the existing credentials of the selected configlets.
Modify Mode	
Old Credential	Old credential appears in clear text in a non-editable text box.

Field	Description
New Credential	Enter the new password of the selected configlets. This field is editable when you select the Modify option.
Confirm Credential	Enter the new password of the selected configlets again to confirm the new value. This field is editable when you select the Modify option.

Step 5 Click **Submit** to record changes.

The changes are reflected in the Editor window.

Step 6 Enter modification comments in the Change Description field.

Removing a Configuration File

You can use this feature to remove configuration files from a private work area or a public work area using Config Editor.

To remove a configuration file stored in the private work area:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs**.

The List of Private Configs window appears.

Step 2 Select the configuration files that need to be removed.

Step 3 Click **Delete**.

To remove a configuration file stored in the public work area or the user archive:

Step 1 Select **Configuration > Tools > Config Editor > Public Configs**.

The Public Configs window appears.

Step 2 Select the configuration files that need to be removed.

Step 3 Click **Delete**.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Saving a Configuration File

You can use this feature to save your changes to the configuration file. The changes can be saved in either a private area or a public area. You can open the file later to modify it or to deploy it to the device.

To save a configuration file:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Save**.

The Save Config dialog box appears, only if you are saving the configuration file for the first time. The subsequent saving of a file is done directly to its previously saved location.

Step 4 Enter the information required to save a configuration file.

Field	Description	Usage Notes
Public	Saves the files in the public area.	None.
Private	Saves the files in the private area.	When a configuration from a list of private configs is opened and saved in the public area (user archive) with the same name as the private configuration, the private configuration with that name gets deleted. However, the reverse is not true. That is when a config is opened from the public area (user archive) and saved in the private area, the public configuration is not deleted.
Branch Name	Name of branch.	Private area to where configuration files are stored locally.

Step 5 Click either:

- **Submit** to save the configuration file.

  Or

- **Cancel** to return to the previous setting.

After the configuration file opened from the Device Archive is saved to the private or public archive, all the subsequent operations (compare, show changes) behave as if the configuration is opened from a private or public location.

Undoing All

You can use this feature to undo editing or typing changes. To do this:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Edit the configuration file.

Step 4 Click **Undo All**.

A message window appears with the message:

```
Do you want to discard all the changes?
```

Step 5 Click either:

- **OK** to return to the last saved configuration file.

  Or

- **Cancel** to avoid making any changes.

Replacing All

You can use this feature to search for and replace text in the file. To do this:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Replace All**.

The Replace All dialog box appears.

Step 4 Enter the text to search for in the Find field.

Step 5 Enter the replacement text in the Replace With field.

Step 6 Click either:

- **Replace All** to replace all instances of the text in the text area.

  Or

- **Cancel** to avoid making any changes.

Printing a Configuration File

You can use this feature to print the configuration file. To do this:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Select the Print icon at the top right corner.

A new browser window appears. The details are in PDF format. You can print the information, using the Print option provided by the browser.

Exporting Changes of a Configuration File

You can use this feature to export the modified configuration file to either cfg or XML formats based on the edit operation. To do this:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Select the Export icon at the top right corner.

A new browser window appears to select the directory to which the modified Configfile is exported either in cfg or XML formats.

- If you are using the Raw mode then the exported file format is cfg. The file name convention is *DeviceName-VersionNumber-raw*.cfg.
- If you are using the Processed mode then the exported file format is XML. The file name convention is *DeviceName-VersionNumber-proc*.xml.

Where *DeviceName* is the device Display Name as entered in Device and Credential Repository and *VersionNumber* is the device configuration version.

The default directory where the modified Configuration file is exported is:

On Solaris and Soft Appliance server,

/var/adm/CSCOpx/files/rme/cfgedit/configexport

On Windows server,

NMSROOT\files\rme\cfgedit\configexport

Deploying a Configuration File

You can use this feature to deploy a configuration file to a device.

To deploy a configuration file:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Deploy.**

The Job Option Details dialog box appears.

Step 3 Enter the following information:

Field	Description
Job Information	
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Job Options	
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Admin > Network > Configuration Job Settings > Config Job Policies) either: – Enter the device login user name and password and device Enable password or – Disable the Job Password option in the Job Schedule and Options dialog box.

Field	Description
Deploy Mode	
Overwrite	Select the Overwrite option, if you want to replace the existing running configuration on the device, with the selected configuration. This is the default option for the configuration deployment. The configuration that you have selected is compared with the latest running configuration in the Configuration Archive. (LMS assumes that the latest running configuration in the archive is the same as the configuration currently running on the device.) The Overwrite mode ensures that the running configuration on the device is overwritten with the selected configuration. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same. Overwrite mode supports Write2Run of the configuration only.
Merge	Select the Merge option, if you want to add incremental configuration to the device. The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration. The selected running configuration is not compared with the running configuration in the Configuration Archive. We recommend that you use this option on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device. Merge mode supports both Write2Run and Write2Start of the configuration.

Step 4 Click **Submit**.

An immediate Deploy of Configuration on Device job will be scheduled.

A message appears, `Job` *ID* `is created successfully`.

Where *ID* is a unique Job number.

Step 5 Click **OK**.

You can check the status of your scheduled *Config Editor Deploy* job by selecting **Configuration** > **Job Browsers** > **Config Editor**.

- Configurations edited from Raw mode (.RAW) can be downloaded to both Startup or Running configuration of the device.
- Configurations edited from Processed mode (.PROC) can only be downloaded to the Running configuration of the device.

Closing a Configuration File

You can use this feature to close the configuration file without exiting the application. If the file contains unsaved changes, you are prompted to save before closing.

To close the configuration file:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Close**.

If the file contains any unsaved changes, a message window appears with the message:

```
You have done some changes since last save. Do you want to the save the changes?
```

Step 4 Click either:

- **OK** to save the configuration file in a private area.

  Your changes are saved.

  Or

- **Cancel** to ignore your changes.

Selecting Configuration Tools

You can use this feature to choose a configuration tool from the list of configuration tools. The list of configuration tools available are as follows:

- Comparing Versions of Configuration Files
- Displaying Your Changes
- Overview: Syntax Checker

To select a configuration tool:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Tools.**

The Select Tool dialog box appears with the following tools:

Option	Description
Compare Config	Compares the current file with any earlier version in the configuration archive.
View Changes	Displays the changes made in the opened file.
External Syntax Checker	1. Select this option to check the configuration file using an external syntax checker that is registered with Cisco Management Integration Center (CMIC). 2. Click **Submit**. Config Editor launches the URL, displaying the configuration commands and sysobject ID of the device as input to the external syntax checker. 3. View the output displayed by the external syntax checker. 4. Modify the commands in Config Editor.

Step 4 Select a tool.

Step 5 Click either:

- **Submit** to launch the tool.

Or

- **Cancel** to close the window.

Comparing Versions of Configuration Files

You can use this feature to compare the current file with any earlier version in the configuration archive.

The Compare option is enabled only if a file is open.

To compare versions of configuration files:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Tools.**

The Select Tool dialog box appears.

Step 4 Select **Compare Config**.

Step 5 Click either:

- **Submit** to view the Version Selector dialog box and proceed to the next step.

  Or

- **Cancel** to close the window without making any changes.

Step 6 Select a version with which you want to compare the current open file, from the list of other versions.

The Configuration Compare Report appears.

Step 7 Select the View mode.

Step 8 Click **Processed** to display files in Processed mode. This is the default option.

Files appear at the configlet level (a set of related configuration commands).

Step 9 Click **Raw** to display the files in Raw mode.

The entire file appears.

If you want to print the report, click **Print**.

You can select Diff only option to view the differences, or All to view the entire configurations and compare the differences.

Displaying Your Changes

You can use this feature to display the changes made in the opened file. The text file in archive is compared with the opened version.

The View Changes option is enabled only if a file is open

To display the changes in the open file:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing based on Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Tools**.

The Select Tool dialog box appears.

Step 4 Select **View Changes** option.

Step 5 Click either:

- **Submit** to view the differences in a new window.

Or

- **Cancel** to close the window without making any changes.

Overview: Syntax Checker

Config Editor provides ways to check the syntax of config commands using syntax checker. Config Editor checks syntax using the Interface to External Syntax Checker.

Interface to External Syntax Checker

The external syntax checker has to be registered with Cisco Management Integration Center (CMIC) using Link Registration.

For details see, Registering an External Syntax Checker Application With CMIC. Config Editor queries CMIC to check if the application is registered with the name “Config Syntax Checker”.

If the application is registered, Config Editor knows the External Syntax Checker URL to be launched and parameters to be passed to the syntax checker.

Config Editor launches the URL with two parameters, deviceSysObjID and cfgCmds:

- **deviceSysObjID**—sysObjectID of the device. External Syntax Checker uses deviceSysObjID to identify the device type.
- **cfgCmds**—List of commands for which the syntax has been checked.

ConfigEditor launches the External Syntax Checker URL in POST method. When the URL is launched you can view the configuration commands for which the syntax has been checked.

To validate the results and correct the commands in Config Editor:

Step 1 Select **Configuration > Tools > Config Editor > Config Editor**.

Step 2 Select **Device and Version** in the Selection Area page.

Step 3 Click **Go**.

The Device and Version dialog box appears.

Step 4 Select the required device using Device Selector.

Step 5 Select the information required to open a configuration file.

Field	Description
Version	
Latest	Select the latest version of the configuration file.
Earlier	Select an earlier version of the configuration file.
Version Number	Version number of the configuration file. This option is enabled when you select **Earlier** in the version field. This field is not editable. To enter the version number: 1. Click **Select** to open the Version Tree dialog box. 2. Select the desired version. 3. Either: – Click **OK** to select the version Or – Click **Cancel** to close the window.

Step 6 Click **Edit** to edit a configuration file

The Configuration Editor dialog box appears.

Step 7 Click **Tools.**

The Select Tool dialog box appears with the tools.

Step 8 Select **External Syntax Checker**.

Step 9 Click **Submit** to launch the tool.

Config Editor launches the External Syntax Checker URL.

Registering an External Syntax Checker Application With CMIC

To register an external syntax checker application with CMIC (Cisco Management Integration Center):

Step 1 Select **Link Registration**.

The Registered Links window appears.

Step 2 Click **Registration** in the Links Registrations Status page.

The Enter Link Attributes window appears.

Step 3 Enter the inputs for the following fields:

Field	User Notes
Name	Enter Config Syntax Checker.
URL	Enter the External Syntax Checker URL.
Display Location	Select Third Party.

The Registered Links window appears with the list of registered links.

Viewing the List of Modified Configs

You can use this feature to display a list of configuration files modified by any user in a private work area (select **Private Configs**) or a public work area (select **Public Configs**).

To list out all the modified files:

Step 1 Select **Configuration > Tools > Config Editor > Private Configs** to open a configuration file stored in a private work area.

The List of Private Configs window appears.

Or

Select **Configuration > Tools > Config Editor > Public Configs** to open a configuration file stored in a public work area.

The Public Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Do any of the following:

- Select the file and click **Edit** to edit an opened configuration file.

  The Configuration Editor dialog box appears.
- Select the file and click **Deploy** to deploy a job.

  The Select Configs dialog box appears.
- Select the file and click **Delete** to remove an opened configuration file.

  The screen is refreshed and the file is removed.

You can open a raw config in processed format. However, you cannot open a processed config in raw format.

Overview: Opening a Configuration File

You can use this feature to open a configuration file for editing.

You can open a configuration file by:

- Device and Version—Opens a configuration file from the archive.
- Pattern Search—Opens a configuration file by searching for a pattern.
- Baseline—Opens a configuration file using a baseline template stored in the device configuration management repository.
- External Location—Opens a configuration file stored in an external location

If another user has opened the configuration file, config editor opens another copy of the file.

To open a configuration file:

Step 1 Select **Configuration > Tools > Config Editor > Config Editor**.

Step 2 Select an option in the Selection Area page.

Step 3 Click **Go.**

The Option dialog box opens in a new window.

Opening a Configuration File - By Device and Version

You can use this feature to open a configuration file from the archive. The file opens in read-write mode depending on your edit permissions.

The file appears in either the Raw or Processed mode, based on your preferences.

To open a configuration file from the archive:

Step 1 Select **Configuration > Tools > Config Editor > Config Editor.**

Step 2 Select **Device and Version** in the Selection Area page.

Step 3 Click **Go**.

The Device and Version dialog box appears.

Step 4 Select the required device using the Device Selector.

Step 5 Select the information required to open a configuration file.

Field	Description
Version	
Latest	Select the latest version of the configuration file.
Other	Select an earlier version of the configuration file.
Version Number	Version number of the configuration file. This option is enabled when you select **Other** in the version field. This field is not editable. To enter the version number: 1. Click **Select** to open the Version Tree dialog box. 2. Select the version you need. 3. Either: • Click **OK** to select the version Or • Click **Cancel** to close the window.
Format	
Raw	Displays the entire configuration file. After you open a file in a specific mode, you can view it only in that mode.
Processed	Displays only the commands.

Step 6 Click either:

- **Edit** to edit a configuration file

  The configuration editor dialog box appears.

Or

- **Reset** to clear all fields and get to the default setting.

Opening a Configuration File - By Pattern Search

You can use this feature to open a configuration file by

- Selecting a label set in Config Archive
- Selecting a custom query of default patterns
- Searching for a pattern.

A pattern can be any text string. The file is displayed in either the Raw or Processed mode, based on your preferences.

To open a configuration file:

Step 1 Select **Configuration > Tools > Config Editor > Config Editor**.

Step 2 Select **Pattern Search** in the Selection Area page.

Step 3 Click **Go**.

The Pattern Search dialog box appears.

Step 4 Do any of the following:

- Open a configuration file by selecting a label set in Config Archive. See Configuring Labels for more information.
- Open a configuration file by selecting a custom query of default pattern
- Open a configuration file by searching for a pattern

Open a configuration file by selecting a label set in Config Archive. See **Configuring Labels** for more information.

a. Select **Label** to enable the Select a Config Label drop-down list box

b. Select the required label from the Select a Config Label drop-down list box

If you select a label and some devices from the Device Selector, and click **Search**, the search results will only be for the devices that are part of the selected label.

Open a configuration file by selecting a custom query of default pattern

Select the required **Custom Query** from the Select Custom Query drop-down list box. To create a custom query, select **Configuration > Configuration Archive > Views > Custom Queries**.

Open a configuration file by searching for a pattern

a. Enter a pattern in the editable Pattern Column. For example, `http server`.

To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields and so on. You cannot search for special characters. For example, control-C.

b. Click the corresponding Contains/Does not contain row to view the selection drop-down list box.

c. Select **Include** if you wish to search for configurations that match the patterns you entered and select **Exclude** if you wish to search for configurations that do *not* match the patterns you entered. Select the required devices using the Device Selector.

Step 5 Select the required options:

Field	Description
Setting	
Match Any	Searches for configurations that have at least one of the patterns you entered.
Match All	Searches for configurations that include all patterns you entered.
Match Case	Searches for configurations that are identical to the pattern entered.
Search Versions	
Latest	Searches in the latest version of the configuration file
All	Searches in all the versions of the configuration file

Step 6 Click **Search**.

The Search Archive Result window appears in the Pattern Search Results page with the search results. The columns in this window are:

Column	Description
Device Name	Name of the device
Version	Version of the configuration file
Created On	Date on which the configuration file was created
Change Description	Modification comments

Step 7 Select any of the following:

- **Edit** to open the selected configuration file in a pop up window for editing. The search result page will be retained. You can select another configuration from the search result page and open that file too for editing.
- **Back** to return to the Pattern Search page.
- **Finish** to complete the search.
- **Cancel** to return to the Selection Criteria page.

Opening a Configuration File - By Baseline

You can use this feature to open a baseline configuration template maintained in the configuration archive. You can create a baseline configuration from the baseline template by replacing all the variables that appear in the configuration.

Config Editor does not check whether you have changed the template variables.

Note The baseline template will be opened only in Raw format.

To open a baseline configuration template:

Step 1 Select **Configuration > Tools > Config Editor > Config Editor**.

Step 2 Select **Baseline** in the Selection Area page.

Step 3 Click **Go**.

The Baseline Config dialog box appears.

Step 4 Select the required devices using the Device Selector.

Step 5 Click **Next**

The Baseline Template window appears with the following details:

Column	Description
Baseline Name	Name of the Baseline template.
Description	Brief description about the template.
Created On	Date on which the template was created.

Step 6 Select a Baseline template based on the device type.

Step 7 Select any of the following:

- **Back** to return to the Baseline Config page.
- **Finish** to associate the selected template to a device.
- **Cancel** to return to the Selection Criteria page.

While editing a baseline template, you are required to replace variables that appear in the template with actual values.

```
For example, in the following line [msg] is the variable.
banner motd [msg]
```

You should replace `[msg]` with actual value.

Baseline Configuration Editor

You can use this feature to edit the Baseline template of the configuration file. To do this:

Step 1 Select **Configuration** > **Tools** > **Config Editor** > **Config Editor**.

Step 2 Select **Baseline** in the Selection Area page.

Step 3 Click **Go**.

The Baseline Config dialog box appears.

Step 4 Select the required devices using the Device Selector.

Step 5 Click **Next**.

The Baseline Template window appears with the following details:

Column	Description
Baseline Name	Name of the Baseline template.
Description	Brief description about the template.
Created On	Date on which the template was created.

Step 6 Select a Baseline template based on the device type.

Step 7 Click **Finish**.

The Baseline Configuration Editor dialog box appears.

Step 8 Edit the text area. (The upper section contains only non-credential commands and is called the text area.)

Step 9 Enter comments for changes in baseline in the Change Description field.

Step 10 Select any of the following:

- **Save** to save changes to the configuration file.
- **Undo All** to undo editing or typing changes.
- **Replace All** to replace a string in the opened configuration files.
- **Tools...** to launch the Config Editor tools.
- **Close** to close the Config Editor window.

Opening an External Configuration File

You can use this feature to associate a device with the selected configuration file from an external location (other than archive) in the server. The file appears in either a Raw or Processed mode, based on your preferences.

For example, if you associate the selected configuration to an IOS device in the Processed mode, then the given configuration is processed based on the IOS rules defined in LMS.

The file in the archive can be opened with a specified format from the temp directory on the local server, from another file system mapped drive or any mount. The file opened is validated for format with DCMA.

To open a configuration file from an external location:

Step 1 Select **Configuration > Tools > Config Editor > Config Editor**.

Step 2 Select **External Location** in the Selection Area page.

Step 3 Click **Go**.

The External File Selection dialog box appears.

Step 4 Click **Browse** to select the external file location.

The External Config Selector dialog box appears with the following fields:

Field	Description	Usage Notes
File	Location of the file	Enter the file location. For example, D:/CSCOpx
Directory content	Name of the directory	Select the directory. For example, bin/
Drive	Name of the drive	Select the drive. For example, D:\

Step 5 Click either:

- **OK** to enter the external location.

  Or

- **Cancel** to return to the External File Selection page.

Step 6 Select the required devices using the Device Selector.

Step 7 Either:

- Click **Edit** to edit a configuration file

  The configuration editor dialog box appears.

  Or

- Click **Reset** to clear all fields and get to the default setting.

You can control the access to directories/folders present on the server. There is a property file for this purpose located at:

- *NMSROOT*/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/config/cfgedit /ConfigEditor.properties (On Solaris and Soft Appliance)
- *NMSROOT*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\config\cfgedit \ConfigEditor.properties (On Windows)

NMSROOT is the LMS install directory.

This file has two variables:

- *DIR_LIST*—You can mention all the directories or files separated by pipe symbol (|).
- *ALLOW*—You can set as true or false. If you set the value as true, you can access only those directories or files given as values for the variable *DIR_LIST*. If you set the value as false, you cannot access those directories or files given as values for the variable *DIR_LIST*.

The default values for the variables are:

- *DIR_LIST*—`etc/passwd`
- *ALLOW*—`false`

Configuration Deployment in Overwrite and Merge Modes

Overwrite Mode

Config Editor assumes that the latest archived version is the same as the running configuration on the device.

Before Config Editor downloads the archived configuration on the device, it compares the archived version (which you have modified) with the latest version. The application then overwrites the running configuration on the device with the archived version. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same.

For example, assume that the archived version contains commands a, b, c, and d; and that the latest running version, contains commands a, b, e, f, and g. After the archived configuration has been restored, the running configuration on the device, will contain commands a, b, c, and d.

Ensure that all the required commands are in the archived version. You can review the work order and make necessary changes by editing the archived version, if required.

This is the default mode for the configuration deployment.

Merge Mode

The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration.

The selected running configuration is not compared with the running configuration in the Configuration Archive.

We recommend that you use this mode on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device.

Overview: Downloading a Configuration File

To download a configuration file to the device and to the archive, you must:

- Create a download job.
- Select the configuration file on which the job will run.
- Configure the job properties.
- Set the job approvers.
- Review the job work order.

When a job starts to download, the users on the job approver list are notified by e-mail. At least one approver must approve the job before it can run. Make sure that an approver list with the approvers you want exists.

If there is no approver list but you have the correct access privileges, you must modify or create approver lists, using the Job Approval option. Otherwise, contact your system administrator. See *Administration of Cisco Prime LAN Management Solution 4.1* for more information.

Starting a New Download Job

You can use the Create Config Download Job wizard to define and schedule a download job.

Step 1 Select **Configuration > Job Browsers > Config Editor**.

The Config Deploy Job Browser window appears.

Step 2 Click **Create**.

The Create Config Download Job wizard appears.

All dialog boxes of the wizard contain the following buttons:

Button	Description
Back	Returns to the previous page.
Next	Returns to the next page.
Finish	Completes creation of jobs.
Cancel	Cancels creation of job.

Selecting Configs

You can use the Select Configs dialog box to select configuration files of devices on which the download job will run.

You must start a new download job before you start selecting configuration files. To do this:

Step 1 Select a configuration file on which to run the job using device selector on the left pane.

The select configuration file dialog has two panes.

- Left Pane—The Device Selector appears.
- Right Pane—The list of selected configuration files appear.

Step 2 Click either:

- **Add Latest** to move the latest version of the selected configuration file to the Selected Configuration Files pane

  Or

- **Add Other Version** to move any version of the selected configuration file to the Selected Configuration Files pane

Step 3 Do any of the following:

- Click **Next** to proceed to the Job Schedule and Options dialog box.
- Click **Cancel** to stop creating a download job.
- Select a configuration file from the Selected Configuration Files pane and click **Delete** to remove a configuration file.

Scheduling a Job

This feature allows you to assign a job name, schedule the job and set job options.

Before scheduling a job you must:

1. Start a new download job.
2. Select Configs.

To schedule a job:

Step 1 Enter the following information in the Job Schedule and Options dialog box.

Field	Description/Action	Usage Notes
Scheduling		
Run Type	Schedules the job to run immediately or in the future. Select either **Once** or **Immediately**.	You can specify when you want to run the job. To define this, select an option from the drop down menu: • **Once**—Job will run once in the future. You can specify the Starting Date and Time for the job to be run • **Immediately**—Job will run immediately. This option is not available if Job Approval is enabled.
Date	Date on which you want to run the job.	Select date for the job to run. If Run Type is Immediate, the system date is automatically selected.
At	Time when you want to run the job in the future.	Select time for the job to run. If Run Type is Immediate, the system time is automatically selected.
Job Info		
Job Description	Enter job description.	Make each description unique so you can easily identify jobs.
E-mail	Allows you to enter the e-mail addresses to which the job will send status notices. Separate multiple addresses with commas.	E-mail notification is sent when job is created, started, deleted, canceled, and completed.
Comments	Allows you to enter comments.	
Approval Comment	Allows you to enter approval comments.	This field is not active if approval comments were not set using administration approval. Select Configuration > Config Jobs > Job Approval to set approval comments. For more information, see *Administration of Cisco Prime LAN Management Solution 4.1*.

Field	Description/Action	Usage Notes
Maker E-mail	Mail ID of the person who created the job.	This field is not active if approvers were not set using administration approval. Select Configuration > Config Jobs > Job Approval to set approval comments. For more information, see *Administration of Cisco Prime LAN Management Solution 4.1*.
Job Options		
Fail on mismatch of Configuration Version	Select this option, if you want to cause the job to be considered Failed, if there is a version mismatch.	A job is considered Failed when the most recent configuration version in the configuration archive is not identical to the configuration that was running when you created the job.
Sync archive before running a job	Select this option if you want to archive the running configuration before making configuration changes.	Synchronize archive before running a job policy gets selected when Fail on mismatch of Configuration Version policy is selected.
Delete Config after Download	Select this option if you want to delete the configuration file after download.	Applicable only to private configuration files.
Copy running to Startup	Select this option if you want to copy the running configuration to the startup configuration on each device after configuration changes are made successfully.	This does not apply to Catalyst OS devices.
Enable Job Password	Select this option to enable username and password.	
Login User Name	Enter the username configured on the device.	This field is editable only when you select the Enable Job Password option. LMS ignores the username in the database and uses the newly entered username instead.
Login Password	Enter the password for the device.	This field is editable only when you select the Enable Job Password option. LMS ignores the password in the database and uses the newly entered password instead.
Enable Password	Enter the enable password configured on the device.	This field is editable only when you select the Enable Job Password option. LMS ignores the password in the database and uses the newly entered password instead.

Field	Description/Action	Usage Notes
Failure Policy	Specify what the job should do if it fails to run on the device.	• Select **Ignore Failure and Continue** from the drop-down list box to continue the job and make configuration changes to the remaining devices, configured by the job Or • Select **Stop on Failure** to stop making changes to the remaining devices.
Execution	Mode in which the job is executed. There are two options, Parallel and Sequential.	1. Select **Parallel** to run the job on multiple devices at same time Or Select **Sequential** to run the job one device at a time. 2. Click **Device Order.** The Set Device Order dialog box appears. 3. Use the Up and Down arrows to move a device up or down. 4. Click **Done**.
Deploy Mode	Mode in which the configuration file is downloaded. The two modes are Overwrite and Merge.	Do either of the following: • Select the Overwrite option, if you want to replace the existing running configuration on the device, with the selected configuration. This is the default option for the configuration deployment. The configuration that you have selected is compared with the latest running configuration in the Configuration Archive. (LMS assumes that the latest running configuration in the archive is the same as the configuration currently running on the device.) The Overwrite mode ensures that the running configuration on the device is overwritten with the selected configuration. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same. Overwrite mode supports only Write2Run of the configuration. Or • Select the Merge option, if you want to add incremental configuration to the device. The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration. The selected running configuration is not compared with the running configuration in the Configuration Archive. We recommend that you use this option on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device. Merge mode supports both Write2Run and Write2Start of the configuration.

Field	Description/Action	Usage Notes
Write To	The method in which the Configuration is pushed. The two methods are Running and Startup	Do either of the following: • Select the Running option, if you want to replace the existing running configuration on the device, with the selected configuration file. This is also referred to as Write2Run. Or • Select the Startup option, if you want to erase the contents of the device's startup configuration and write the contents of the given file as the device's new startup configuration. This is also referred to as Write2Start. Configurations edited from Raw mode (.RAW) can be downloaded to both Startup or Running configuration of the device. Configurations edited from Processed mode (.PROC) can only be downloaded to the Running configuration of the device.
Update credentials after deploy	Update the credentials in DCR after deployment, if the deployed commands include any credentials commands.	Choose this option if you want to update the DCR with the deployed credentials commands such as SNMP community strings, Telnet username/password etc. Write2Start does not support changing the credentials after deployment.

Step 2 Select any of the following:

- **Back** to return to the Select Configs dialog box.
- **Next** to proceed to the Job Summary dialog box.
- **Cancel** to stop creating a Download job.

Reviewing the Work Order

The work order summarizes the job you created. If you find any changes missing when you review the work order you can go back and change the options.

Complete the following prerequisite steps of the job definition process:

1. Start a new download job
2. Select configs
3. Configure job properties
4. Set job approvers, if Job Approval is enabled

To review the work order:

Step 1 Review the information in the Work Order dialog box. The fields in this dialog box are:

Field	Description
General Info	Detailed information about the job, such as owner, description and schedule.
Job Approval Info	Status of approval.
Job Policies	Policies configured for the job. Edit in Job Properties dialog box.
Devices	Devices on which the job will run. Edit in Device Selector dialog box.
Device Commands	Commands that the job will run.
Username	Username of the job owner.

- To modify the job, return to any previous dialog box and change the information.
- To return to a previous dialog box, click **Back** until the dialog box appears.

Step 2 Click **Finish** in the Work Order dialog box to register the job.

Viewing the Status of all Deployed Jobs

You can use this feature to view the status of all pending, running, and completed jobs. You can create a new job or edit, copy, stop and delete a job that you have opened.

You can only Edit one job at a time while you can Stop or Delete multiple jobs at a time.

To view all the downloaded jobs:

Step 1 Select **Configuration > Job Browsers > Config Editor**.

The List of Deploy Jobs window appears with the list of all the jobs.

Column	Description
Job ID	Unique number assigned to job at creation. Never reused.
Run Status	Job states: • Canceled • Suspended • Missed start • Rejected • Succeeded • Succeeded with info • Failed, Crashed • Failed at start • Running.
Description	Description of the job, as entered during job definition.
Owner	Name of the user who owns the configuration file.
Scheduled On	Date and time the job is scheduled to run.
Completed At	Date and time at which the job is completed.
Schedule Type	Job schedule types: • Suspended • Scheduled • Waiting for approval • Rejected • Canceled.
Status	Status of running or completed jobs: Job Started, Progress, Job Cancelled, Job Failed, Job Successful. Pending jobs have no status.

Step 2 Click one of the following buttons:

Button	Description	Usage Notes
Create	Creates a new job.	1. Click **Create**. The Create Config Deploy Job wizard appears. 2. Use the wizard to define and schedule a download job.
Edit	Edits pending job. The Job definition opens with the current information, including Job ID. You can edit the job in the same way as you can define and schedule a new job.	Click **Edit** to edit only jobs you own. If the job start time occurs during editing, it will run without the edits. In such a case, you can complete your edits, reschedule the job, and re-edit it. To prevent job from running unedited: 1. Complete edits before job start time. 2. Cancel job and create new one.
Copy	Copies job. You can edit the job in the same way as you can define and schedule a new job.	Click **Copy**. The Job definition opens with the current information and the new ID except job schedule details filled in.
Stop	Stops a running job.	1. Click **Stop**. You are prompted to confirm stopping a job. 2. Click **OK.** You can stop only the jobs that you own. Admin level users can stop all jobs.
Delete	Removes the job from the Job Scheduler.	1. Click **Delete**. You are prompted to confirm stopping a job. 2. Click **OK** or **Cancel**. You can remove only the jobs that you own. Admin level users can remove all jobs.

CHAPTER 8

Managing Software Images Using Software Management

Manually upgrading your devices to the latest software version can be an error-prone, and time-consuming process. To ensure rapid, reliable software upgrades, Software Management automates the steps associated with upgrade planning, scheduling, downloading, and monitoring.

This section contains:

- Setting Up Your Environment
- Software Repository
- Software Distribution
- Using Software Management Job Browser
- Understanding User-supplied Scripts
- Locating Software Management Files

Using Software Management, you can:

- Set up your Software Management preferences.

  You can specify information such as the directory where images are stored, and the pathname of the user-supplied script to run before and after each device software upgrade.

  You can enable and define the protocol order for Software Management tasks. You can also enable the Job Based Password option for Software Management tasks.

  You can specify if the images on Cisco.com should be included during image recommendation of the device. Also specify the Cisco.com filters so that only the images that match the filter criteria are selected.

- Analyze software upgrades

  You can generate Upgrade Analysis reports that help you determine prerequisites for a new software deployment.

  These reports analyze the proposed images to determine the hardware upgrades (device access, boot ROM, Flash memory, RAM, and NVRAM and boot Flash, if applicable) required before you can perform the software upgrade.

  See Upgrade Analysis for further details.

- Perform In Service Software Upgrade (ISSU)

  LMS supports the In Service Software Upgrade (ISSU) process that allows Cisco IOS software images to be updated without rebooting the device. This process increases network availability and reduces downtime caused by planned software upgrades.

  See Support for In Service Software Upgrade for further details.

- Import images into the software repository

  You can determine the images missing from your repository and import them into the software repository.

  You can also keep the repository up-to-date and periodically synchronize the repository with the images running on your network devices.

  You can also schedule an image import for a later, more convenient time.

  See Adding Images to the Software Repository for further details.

- Distribute software images to groups 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 groups and search criteria. You can also use some other selection criterion, such as the current software version or hardware type to specify the groups.

  You can run the device upgrades job sequentially or in parallel. After upgrading the devices, you can also specify the reboot order.

  See Software Distribution for further details.

- Distribute images as patches to group of devices

  Depending on system complexity, you can configure upgrades for groups of devices to the patch software images.

  You can specify these groups manually, using your groups and search criteria. You can also use some 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.

  See Patch Distribution for further details.

- Reduce errors by using a recommended image

  Software Management checks the current software version, Flash device size, DRAM size, boot ROM version. Software Management also checks any device type specific software and hardware requirements for compatibility. Software Management checks and recommends a best-fit image for a device.

  See Understanding Upgrade Recommendations for further details.

- Schedule image upgrade jobs

  You can schedule image upgrades to occur immediately or at a later, more convenient time. Optionally, you can integrate software upgrade scheduling into your internal change approval process.

  After an upgrade, you can:

  – Undo the upgrade and roll back to the previous image

    Software Management tracks the image history of each device so that if you upgrade to a new image, you have a record of what has been installed on the device. This information allows you to undo the upgrade and roll back to the previous image, if necessary.

A Change Audit record is logged for this task. You can generate the Standard Change Audit report. See *Reports Management with Cisco Prime LAN Management Solution 4.1* for more information.

See Undo a Successful Distribution Job for further details.

– Retry the upgrade on devices that failed in a previous job

You can also retry a job for devices that failed the upgrade process. For example, you may need to do this because of a configuration error or a bad network connection.

You can retry the job and include only those devices that were not upgraded previously.

See Retry a Failed Distribution Job for further details.

- Track job progress and job history information

  Software Management generates detailed job reports. These reports display the status of each software upgrade and a detailed job log. They also keep track of job and device operations and job history information.

  See Using Software Management Job Browser for further details.

- Track software bugs

  You can view the known catastrophic or severe bugs in the software running on the devices supported by Software Management using Locate Device Report (**Reports > Cisco.com > Locate Device Report**).

  See *Reports Management with Cisco Prime LAN Management Solution 4.1* for further details.

- Set the debug mode for Software Management application

  You can set the debug mode for Software Management application in the Log Level Settings dialog box (**Admin > System > Debug Settings > Config and Image Management Debugging settings**).

  See *Administration of Cisco Prime LAN Management Solution 4.1* for further details.

- The supported IOS image version is 11.x and later.

For list of supported devices in the Software Management application, see:

- Supported Image Import Features for Software Management

  http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

- Supported Image Distribution Features for Software Management

  http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

Setting Up Your Environment

This section lists all prerequisites for using the Software Management in LMS.

- Requirements on LMS Server
- Logging Into Cisco.com
- Configuring Devices for Upgrades
- Using Job Approval for Software Management

Requirements on LMS Server

The following are the prerequisites:

- Make sure you have a directory or file system location with enough space to store the software images.
- Verify that you have the appropriate privilege level to access Software Management options. You can view the Permission Report (**Reports > System > Users > Permission**) to know the various privilege levels.
- 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.
- If your system is behind a firewall, configure the proxy URL to access the Internet from the installed system. You can do this using **Admin > System > Cisco.com Settings > Proxy Server Setup.**

  You can enter Cisco.com credentials when you use the Software Management tasks.

  See Logging Into Cisco.com for further details.

Mandatory Setup Tasks

- Add the device passwords to the Device and Credentials database. You can add these credentials using **Inventory > Device Administration > Add / Import / Manage Devices**. Also, see Configuring Telnet and SSH Access for further details.
- Use the **Admin > System > System Preferences** option to enter the name of your SMTP server. You have to configure the SMTP server to send e-mails.

  We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
- If you plan to enable a remote file copy (RCP) or secure copy server as the active file transfer server, see Configuring RCP or Configuring SCP for further details.
- Set or change your Software Management preferences. See *Administration of Cisco Prime LAN Management Solution 4.1* for further details.

Optional Setup Tasks

- Make a baseline of your network images by importing images from the Software Management-supported devices in your network into your software image repository.

  To do this, go to **Configuration > Tools > Software Image Management > Software Repository** and click **Add** and select **Device**.
- Schedule the Synchronization report to run periodically. This is used to determine whether any images running on Software Management-supported devices are not in the software image repository.

  To generate the report, go to **Configuration > Tools > Software Image Management > Repository Synchronization**.
- If you use the Job Approval option to approve or reject jobs, you must create one or more approver lists and enable Job Approval. See *Administration of Cisco Prime LAN Management Solution 4.1* to enable Job Approval.

Logging Into Cisco.com

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 download the cryptographic images on Cisco.com through Software Management tasks, you must have a Cisco.com account with cryptographic access.

To get the 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

After getting the Cisco.com account:

Step 1 Go to the following URL: http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y

The Enter Network Password dialog box appears.

Step 2 Log in with your Cisco.com account.

The Encryption Software Export Distribution Authorization Form page appears.

Step 3 Select your software from the list box and click **Submit**.

The Encryption Software Export Distribution Authorization Form appears.

Step 4 Review and complete the Encryption Software Export Distribution Authorization form and click **Submit**.

The `Cisco Encryption Software: Crypto Access Granted` message appears.

Note It takes approximately 4 hours to process your application. You cannot download the software until the entitlement process is complete. You will not receive any notification for this.

On LMS Server, you can enter Cisco.com credentials for Individual user Cisco.com credentials.

You can enter your individual Cisco.com credentials when you perform any Software Management tasks that need access to the Cisco.com server.

If your Cisco.com username and password have not been added to the LMS database, enter your Cisco.com username and password. If you enter Cisco.com credentials in this workflow, the credentials are valid only for that session.

If your Cisco.com username and password have been added to the LMS database, then Cisco.com login dialog box appears with the information that is available in the LMS database.

If you are accessing Cisco.com over a proxy server, you must enter the proxy server details in the Proxy Server Setup dialog box (**Admin > System > Cisco.com Settings > Proxy Server Setup**).

Using Job Approval for Software Management

You can enable Job Approval for Software Management tasks, (**Configuration > Job Browsers > Job Approval**), which means all jobs require approval before they can run.

Only users with Approver permissions can approve Software Management jobs. Jobs must be approved before they can run if Job Approval is enabled on the system.

The following Software Management tasks require approval if you have enabled Job Approval:

- Adding images to Software Repository (**Configuration > Tools > Software Image Management > Software Repository > Add**) using:
  - Cisco.com
  - Device
  - URL
  - Network (Use Out-of-sync Report)
- Distributing software images **(Configuration > Tools > Software Image Management > Software Distribution**) using any one of these methods:
  - Distributing by Devices [Basic]
  - Distributing by Devices [Advanced]
  - Distributing by Images
  - Remote Staging and Distribution

If you have enabled Approval for Software Management tasks, then in the Job Schedule and Options dialog box, you get these two options:

- Maker Comments—Approval comments for the job approver.
- Maker E-Mail—E-mail ID of the job creator.

See *Administration of Cisco Prime LAN Management Solution 4.1* for more details on creating and editing approver lists, assigning approver lists, setting up Job Approval, and approving and rejecting jobs.

Software Repository

The Software Repository Management window displays the images that are available in the Software Management repository.

This section contains:

- Searching for Images from Software Repository
- Software Image Attributes

The Software Repository Management window contains the following fields, buttons, and the entry in the TOC:

- Software Repository Management Window Fields
- Software Repository Management Window Buttons and TOC Entry

Table 8-1 Software Repository Management Window Fields

Fields	Description
File Name	File name of the software image. Click on the File Name to edit the image attributes. See Editing and Viewing the Image Attributes.
Image Family	Name of the image family.
Image Type	Type of the images (SYSTEM_SW, SUPERVISOR, SUPERVISOR2_6000, SUPERVISOR6000, BOOT_LOADER, ATM_WBPVC, etc.).
Version	Software version number.
Size	Image size in megabytes.
Status	Status of the image on Cisco.com. See Synchronizing Software Image Status With Cisco.com.
Updated at	Date and time the image was checked into the repository.
Comments	Comments, typically used to track the reason for adding the image to the repository.

Table 8-2 lists and describes the buttons and TOC entries in the Software Repository Management Window.

Table 8-2 Software Repository Management Window Buttons and TOC Entry

Buttons and TOC Entry	Description
Software Repository Synchronization (TOC entry)	Keep the software repository up to date. See: • Software Repository Synchronization • Scheduling a Synchronization Report • Viewing a Synchronization Report • Removing a Synchronization Report Job
Filter (Button)	Filter and search images. See Searching for Images from Software Repository.
Add (Button)	Add images to the repository. See Adding Images to the Software Repository.

Table 8-2 Software Repository Management Window Buttons and TOC Entry (continued)

Buttons and TOC Entry	Description
Delete (Button)	Delete images from the repository. See Deleting Images From the Software Repository.
Export (Button)	Export images from Repository. See Exporting Images from Software Repository.
Update Status (Button)	Update the status of the images. See Synchronizing Software Image Status With Cisco.com.

Software Repository Synchronization

The Synchronization report shows the Software Management-supported devices that are running software images not available in the software image repository.

Using this option you can view and schedule the synchronization report.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Select **Configuration > Tools > Software Image Management > Software Repository Synchronization**.

The Software Repository Synchronization dialog box that appears contains the following:

Table 8-3 Software Repository Synchronization Dialog Box

Fields/Buttons	Description
Job Id	Unique number assigned to the job when it is created.
Next Run	Time and date of the next instance of Synchronization Report job.
View Report	You can view the synchronization report. This report displays the Software Management-supported devices that are running software images not available in the software image repository. See Viewing a Synchronization Report for further details.
Schedule	You can schedule a Synchronization report. You can also reschedule an existing Synchronization report. See Scheduling a Synchronization Report for further details.
Remove Job	You can remove the scheduled synchronization report job. See Removing a Synchronization Report Job for further details.

Scheduling a Synchronization Report

To schedule or reschedule a Synchronization report:

Step 1 Go to **Configuration > Tools > Software Image Management > Software Repository Synchronization**. The Software Repository Synchronization dialog box appears.

Step 2 Click **Schedule**. The Job Schedule for Out-of-sync Report dialog box appears.

Step 3 Enter the following information:

Field	Description
Scheduling	
Run Time	You can specify when you want to run the Image Out-of-Sync Report job. To do this, select one of these options from the drop-down menu: • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not been completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	Select the date and time (hours and minutes) to schedule the job.
Job Info	
Job Description	The system default job description, *SoftwareImages Out Of Synch Repor*t is displayed. You cannot change this description.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.

Step 4 Click **Submit**.

If the job was scheduled successfully, the notification dialog box is displayed with the Job ID. You can check the status of your scheduled synchronization job by selecting **Configuration > Tools > Software Image Management > Jobs**.

Viewing a Synchronization Report

To view a synchronization report:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository Synchronization**.

The Software Repository Synchronization dialog box appears.

Step 2 Click **View Report**.

The Image Out-of-sync Report window appears.

Removing a Synchronization Report Job

To remove a Synchronization Report job:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository Synchronization**.

The Software Repository Synchronization dialog box appears.

Step 2 Click **Remove Job**.

A confirmation dialog box shows that the synchronization report job is removed successfully.

Step 3 Click **OK**.

Adding Images to the Software Repository

Your software image repository should contain copies of software images running on all Software Management-supported devices in your network. Use the following options to populate and maintain your software repository:

- Add Image to Software Repository using the Cisco.com option downloads images for devices in LMS from Cisco.com to the software repository.

  See Adding Images to the Software Repository From Cisco.com.

- Add Image to Software Repository using the Device option
  - Imports images from selected Cisco devices to the software repository.
  - Imports software from Flash cards on a live device to the software repository.

  See Adding Images to the Software Repository From Devices.

- Add Image to Software Repository using the File System option imports an image from a directory accessible from the LMS server.

  See Adding Images to the Software Repository From a File System.

- Add Image to Software Repository using the URL option downloads images from the URL you specify.

  See Adding Images to the Software Repository From a URL.

- Add Image to Software Repository using the Network option creates a baseline of all Software Management-supported devices in your network, and imports these images into your software repository.

  See Adding Images to the Software Repository From the Network.

Adding Images to the Software Repository From Cisco.com

Use this option to download software images from Cisco.com into the software image repository.

- Contact your channel partner or enter a request on the main Cisco web site. If you do not have a user account and password on Cisco.com.

  See Logging Into Cisco.com.

- Access the Cisco.com web site to make sure that the releases for the images you plan to download are stable.
- Determine the approximate number and size of the images you want to download. The number of images you can download at a time can vary depending on Cisco.com load, image sizes, network load, and LMS server load.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To add images from Cisco.com:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add**. Do not select any images from Software Repository Management window.

The Image Source dialog box appears.

Step 3 Select **Cisco.com**.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

- Enter your Cisco.com username and password. If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.
- You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

  Admin > System > Cisco.com Settings > Proxy Server Setup

- After entering the credential information, Click **OK**.

Step 4 Click **Next**.

The Device Selection dialog box appears.

Step 5 Select the device from the Device Selection dialog box, and click **Next**.

If you do not want to select any devices, click **Next**.

If you select devices from this list, they identify a subset of device software images. This helps you narrow your options on subsequent screens.

The Add Images from Cisco.com dialog box appears. This dialog box has several sections from which you select combinations of device platforms, software release versions, and software subset images.

See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 6 Select the images to download. Work from left to right and from top to bottom:

a. From the Select a Device/Platform section, select a device or device family.

If you select an individual device, the device family, Cisco IOS release, and required Flash and RAM sizes appear.

For IPX/IGX/BPX/MGX devices, the system software release appears.

A list of available software versions for that device appears in the top middle section.

b. From the Software Versions section, select a software version.

If you are unsure of the subset image you need, see the Release Notes on Cisco.com.

- For IPX/IGX/BPX platforms, both switch software and all applicable module firmware images appear.
- For MGX platforms, system releases appear.

A list of available subset images for the selected software version appear in the top right frame.

c. From the Software Subset Images section, select a subset image.

The subset image is added to the Images to be Added table in the bottom section.

For IPX/IGX/BPX/MGX devices, there are no subset images. Select the item that appears in this section to complete image selection.

Step 7 Continue adding images to the list.

The images that you have added appear in the Images to be Added table. This table contains the following information:

- Devices/Platforms—Name of the device or platform.
- Version—Software version that you have selected.
- Subset—Subset image information.

Step 8 Click **Next** when the list contains all image combinations to download.

Software Management verifies that the images in the Image list run in the selected devices and displays the status in the Add Images from Cisco.com dialog box. The Add Images from Cisco.com dialog box contains:

Field	Description
Device/Platform	Lists the device details that you have selected.
Selected Version and Subset	Displays the image details.
Image Requirements	Displays the required hardware (RAM and Flash) details.

Field	Description
Download	Select the image you want to download. By default, the check boxes are selected for the images that have passed the verification. You can choose not to add an image by deselecting that check box.
Pass/Fail	Results of image verification. • Pass—Device has the minimum required memory and Flash memory. • Fail—Device does not have enough memory or Flash memory. Images that fail verification on one device could work on another. Therefore, you can download a failed image by selecting the Download check box.

Step 9 Select the images to add to the image repository in the Add Images from Cisco.com dialog box and click **Next**.

The Job Control Information dialog box appears.

Step 10 Enter the following in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Import (from Cisco.com) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected **Once** for Run Type, select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter the e-mail address to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter additional information about this job.

Field	Description
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 11 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name that you have selected. It also displays the file size of the image.

Step 12 Click **Finish.**

If the job was scheduled successfully, the notification dialog box appears with the Job ID.

To check the status of your scheduled synchronization job, select **Configuration** > **Tools** > **Software Image Management** > **Jobs**.

.

Adding Images to the Software Repository From Devices

Use this procedure to add software images from Cisco devices to the software repository.

Software Management downloads images from more than one device in parallel. You must ensure that software repository has enough free space to accommodate at least 20 images.

The image import from device option is not available for all the devices. Find the devices from which you can download images in the Supported Image Import Features for the Software Management table on Cisco.com.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

Note View Permission Report (**Reports** > **System** > **Users** > **Permission**) to check if you have the required privileges to perform this task.

To add images from devices:

Step 1 Select **Configuration** > **Tools** > **Software Image Management** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add**.

Do not select any images from Software Repository Management window.

The Image Source dialog box appears.

Step 3 Select **Device**, and click **Next**.

The Device Selection dialog box appears in the Add Images from Device window.

See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

Step 4 Select the devices that contain the images to add to the software repository.

Step 5 Click **Next**.

Software Management retrieves the images, analyzes them according to the selected image type, and displays a report that contains:

Field	Description
Image	Images available on your device.
Available At	Location where the image is available on your device.
Device	Name of the device as managed by LMS.
Size	Image size in bytes.
Errors	Click on the link for details.

By default, the check boxes of the images that are not in the software repository are selected. You can choose not to add an image by deselecting the corresponding check box.

Step 6 Click **Next**.

The Job Control Information dialog box appears.

Step 7 Enter the following in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Import (from Device) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected **Once** for Run Type, select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.

Field	Description
Comments	Enter additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 8 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This description is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name that you have selected. The field also displays the file size of the image.

Step 9 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job select **Configuration > Tools > Software Image Management > Jobs**.

Adding Images to the Software Repository From a File System

Use the following procedure to add software images from a file system to the software repository.

You have to know the directory name in which the image files are stored before importing the images from the File System to the software repository.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To add images from file system:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add**..

Do not select any images from the Software Repository Management window.

The Image Source dialog box appears in the Add Images window.

Step 3 Click **File System**, and click **Next**.

The Add Image From Local File System dialog box appears.

Step 4 Enter the full pathname of the source file or directory.

Or

a. Click **Browse** to search for the directory name.

The Server Side File Browser dialog box appears.

b. Select either the file or the directory on the LMS server.

c. Click **OK**.

Step 5 Click **Next**.

The Image Attributes dialog box appears with this information:

- Filename—Filename as it appears in filesystem directory.

  You cannot add an image if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.

- Image Type—Image type, determined from the filename. If the image type is not correct, select the correct type from the drop-down list box.

  Software Management tries to determine the image type from the filename. If it cannot determine the image type (for example, if the image has been renamed using a nonstandard name), it labels the image type as `Unknown`.

By default, the check boxes of the images that are not in the software repository are selected. You can choose not to add an image by deselecting the corresponding check box.

Step 6 Click **Next**.

The Image Attributes window appears with the following information for verification:

Field	Description	Usage Notes
File Name	Filename as it appears in filesystem directory	You cannot add images if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.
Size	Size of file in bytes.	None.
Image Family	Device family name.	None.
Image Type	Image type, determined from the filename.	Software Management tries to determine the image type from the filename. If it cannot determine the image type (for example, if the image has been renamed to a nonstandard name), it labels the image type as `Unknown`. You must select an image type from an available option before you can add the file to the repository.
Version	Version of the image	None.
Errors	Click on the link for details.	None.

Step 7 Click **Finish**.

A pop up window appears for you to enter a description.

Step 8 Either:

- Click **OK**.

  The Software Repository Management window appears with the newly added images. The description that you have entered appears in the Comments column in the Software Repository Management window.

  Or

- Click **Cancel**.

  The Software Repository Management window appears with the newly added images. The Comments column in the Software Repository Management window will be blank for this task.

Note The import from File System may take more time if you have selected many images.

Adding Images to the Software Repository From a URL

Use the following procedure to add software images from a URL to the software repository.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To add images from URL:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management window appears.

Step 2 Click **Add**.

Do not select any images from the Software Repository Management window.

The Image Source dialog box appears in the Add Images window.

Step 3 Click **URL,** and click **Next**.

The Add Image From URL dialog box appears.

Step 4 Enter the URL details.

For example: http://*servername:portnumber*/file_location/

Where,

- *servername* is the name of the server where the image resides.
- *portnumber* is the http port number.
- *file_location* is the image location on the server. The *file_location* can be swimtemp or htdocs folder.

  For example,

  If the image is in swimtemp, then the URL is http://*servername:portnumber*/swimtemp/image_file

  If the image is in the htdocs, then the URL is http://*servername:portnumber*/image_file

The web server must be running on the destination machine. You can use only HTTP URLs. The remote server should not have any authentication.

Step 5 Click **Next**.

The Job Control Information dialog box appears.

Step 6 Enter the following information in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Import (from URL) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected **Once** for Run Type, select the date and time (hours and minutes) to schedule the job.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You cannot enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 7 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This description is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name that you have selected. It also displays the file size of the image.

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Adding Images to the Software Repository From the Network

This option allows you to import running images from all Software Management-supported devices in your network into the software image repository.

Use this option to create a baseline of the image in your network and populate the software image repository. Use the Synchronize report option to review the Software Management supported devices are running images that are not in the Software Repository.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

You must locate your device in the Supported Image Import Features for Software Management table on Cisco.com. This is because the image baseline capabilities might not be available yet for all devices.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

To add images from network:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add**. Do not select any images from the Software Repository Management window.

The Image Source dialog box appears.

Step 3 Select **Network**, and click **Next**.

Software Management checks the devices on your network and the software images running on those devices.

To run this check faster, select **Use generated Out-of-sync Report** to find the images that are not in the Software Images repository.

You should generate an Out-of-sync Report before selecting this option. The running images in the network that are not in the Software Repository, appear in the Network Baselining dialog box.

If you have not selected the Use generated Out-of-sync Report option, all running images that are not in the Software Repository appear in the Network Baselining dialog box.

The Network Baselining dialog box contains the following information:

Field	Description
File Name	Filename as it appears in filesystem directory. You cannot add an image if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.
Size	Image size in bytes.
Available at	Location where the image is available on your device.
Error	Click on the link to review the details.

By default, the check boxes of the images that are not in the Software Repository are selected. You can choose not to add an image by deselecting the corresponding check box.

Step 4 Select/deselect the images and click **Next**.

The Job Control Information dialog box appears.

Step 5 Enter the following information in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Import (from Network) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected **Once** for Run Type, select the date and time (hours and minutes) to schedule the job.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 6 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This description is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name that you have selected. It also displays the file size of the image.

Step 7 Click **Finish.**

If the job was scheduled successfully, the notification dialog box appears with the Job ID.

To check the status of your scheduled synchronization job, select **Configuration > Tools > Software Image Management > Jobs**.

Synchronizing Software Image Status With Cisco.com

You can check if the software images that are in your software repository are valid images using the Update Status button in the Software Repository Management window.

The Status table column is updated with the following status:

- Not Deferred—Displayed when this image is a valid image.
- Deferred—Displayed when this image is not supported and not available to be downloaded from Cisco.com.

  This image is not recommended by Software Management.
- Software Advisory Notice—Displayed when this image has some issues. You can download this image from Cisco.com.

  This image may be recommended by Software Management. However, you have to read the Software Advisory Notice before importing or upgrading your device.
- Unknown—Displayed when you have added images to the repository for the first time, using any one of these methods:
  - Add Images by Devices
  - Add Images by File system
  - Add Images by URL
  - Add Images from Network

  Use the Update Status button to update the status field.
- Not available—Displayed when information is not available on Cisco.com.

Read the software release notes on Cisco.com for more details.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To synchronize Software Image Status with Cisco.com:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select the images for which you want to know the status and click **Update Status**.

The Cisco.com login dialog box appears.

- If your Cisco.com username and password have not been added to the LMS database, enter your Cisco.com username and password, click **OK**. If you enter Cisco.com credentials in this workflow then the credentials are valid only for that session.
- If your Cisco.com username and password have been added to the LMS database, the Cisco.com login dialog box appears with the information that is available in the LMS database. Click **OK**.

A confirmation message appears that Image Status was retrieved from Cisco.com successfully.

Step 3 Click **OK**.

Review the Status table column in the Software Repository Management window.

Deleting Images From the Software Repository

To delete software images from the software repository:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select the images that you want to delete, then click **Delete**.

A confirmation message appears, `The selected images will be deleted`.

Step 3 Click **OK**.

The Software Repository Management window reappears with the selected images deleted.

Exporting Images from Software Repository

To export software images from the Software Repository:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select images that you want to export, then click **Export**.

A confirmation message appears, `The selected images will be exported`.

Step 3 Click **OK**.

The Select directory to export window appears.

Step 4 Click on **Browse** to select a directory to which you want to export the selected images.

The Server Side File Browser dialog box appears.

Step 5 Choose the required directory and click **OK**.

The Image Directory field in the Select directory to export window displays the directory location that you had selected.

Step 6 Click **Next**

A progress bar appears indicating the progress of the export of images.

The Export Images Summary Report appears, after the image export is completed with the following details:

- Number of Selected Images
- Target Directory
- Summary

Step 7 Click **Finish**.

You have successfully exported the images to the selected directory.

Searching for Images from Software Repository

To search software images from the software repository:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select one of the following from the Filter by drop-down list:

- File Name
- Image Family
- Image Type
- Version
- Size
- Updated At

You cannot use wildcard characters. However, you can filter based on the first character.

For example: If you have images with file names `c3640-i-mz.112-24.P.bin`, `c3640-i-mz.112-25.P.bin`, `cat5000-sup.5-5-18.bin`, and `cat5000-supg.6-4-10.bin`.

If you select File Name as the Filter by option and enter the value as **`c3`**. The filter result displays only `c3640-i-mz.112-24.P.bin` and `c3640-i-mz.112-25.P.bin` images.

Step 3 Click **Filter**.

The Software Repository Management window appears with the filtered image details.

Software Image Attributes

To ensure that Software Management is using the most current information about an image, you should keep the image attributes up to date. Software Management uses image attribute information to:

- Recommend the appropriate image for a given device

  When you distribute an image from the software repository to a device, Software Management uses the image attributes to recommend an image.

- Notify you when a Flash memory or DRAM upgrade is required (upgrade analysis)

  When you distribute an image from the Software Repository to a device, Software Management compares the current Flash memory and DRAM attributes with the Flash memory and DRAM requirements for the new image.

The following sections contain:

- Understanding Software Image Attributes
- Understanding Default Attribute Values
- Finding Missing Attribute Information
- Editing and Viewing the Image Attributes

Understanding Software Image Attributes

To ensure that Software Management is using the most current information about an image, keep the image attributes updated.

If you do not have all the image attribute information when you add the image to the Software Repository, you must edit the attributes when the information becomes available.

Note The auto fill of the Minimum NVRAM, Minimum RAM and Minimum Bootflash image attributes is applicable only for IOS.

The attributes for software images are:

Table 8-4 Software Image Attributes

Attribute	Description	Usage Notes
Minimum RAM	Minimum RAM required.	Select it from the list of options.
Minimum Flash	Minimum Flash memory required.	Select it from the list of options.
Minimum Boot ROM Version	Minimum bootstrap version required.	Enter text in standard Cisco IOS format: a.b(c).
Minimum system software version	Minimum system software version required on the device to upgrade the microcode image (MICA portware, Microcom firmware, CIP microcode only)	Enter text in standard Cisco IOS format: a.b(c).
Minimum supervisor version	Minimum software image version required on supervisor engine module. Cisco Switches can contain any number of modules such as, ATM, FDDI/CDDI, etc. These modules can run different images. There are some interdependencies among the software images that can run on the supervisor engine module and the ATM, FDDI/CDDI, and Token Ring modules residing on the same device chassis.	Enter text in standard Cisco IOS format: a.b(c).
Minimum NVRAM	Minimum NVRAM required to run image on Supervisor Engine III.	Select from list of options.

Understanding Default Attribute Values

The Unknown attribute option has different meanings for different image attributes.

Attribute	Description
RAM	If you select **Unknown**, Software Management computes the RAM value.
Flash Size	If Min.Flash is unknown, it is ignored. If the image size is unknown, the required Flash size to copy the image cannot be determined and the image cannot be used for upgrade.
Boot ROM Version	If you select **Unknown**, no value is stored in this field and the image can run with any boot ROM image version.

Finding Missing Attribute Information

When you import an image from another filesystem, the image might not contain all the attribute information that Software Management requires.

You can find the missing attribute information in the following ways:

- Read the Release Notes on Cisco.com or the documentation CD-ROM.
- Review the image attribute information that is available along with the images, when you download the images from Cisco.com.

You can update the missing attribute information in the Edit/View Image Attributes dialog box.

See Editing and Viewing the Image Attributes for further details.

Editing and Viewing the Image Attributes

LMS allows you to edit and view image attributes.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To edit the software images attributes:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click the **File Name**.

The Edit/View Image Attributes dialog box displays attributes for the selected image type.

Step 3 Make your changes in the available editable fields.

For editable image attributes, you will get either a drop-down list or text fields that you can edit.

Step 4 Either:

- Click **Update,** if you have updated the image attributes.

  The Software Repository Management dialog box appears after updating the attributes.

  Or

- Click **OK,** if you have not updated the image attributes.

  The Software Repository Management dialog box appears without updating the attributes.

Software Distribution

Software Distribution allows you to distribute images in your network and to analyze and determine the impact and prerequisites for new software images before distribution.

This section contains:

Upgrade Analysis

Before planning a software image upgrade, you must determine the prerequisites of the new software images. You can analyze these by using,

- Cisco.com (See Planning an Upgrade From Cisco.com.)
- Repository (See Planning an Upgrade From Repository.)

This section contains:

Planning an Upgrade From Cisco.com

Use the Cisco.com Upgrade Analysis option to determine the impact to and prerequisites for a new software deployment using images that reside in Cisco.com.

This option allows you to identify only images that meet certain criteria. It then analyzes the images to determine the required hardware upgrades (boot ROM, Flash memory, RAM, and access).

This option helps you answer questions such as:

- Does the device have sufficient RAM to hold the new software?
- Have the minimum ROM version requirements been met?
- Is the Flash memory large enough to hold the new software?
- Do I need to add Telnet access information for the device to the Device and Credential Repository?
- Have I performed an upgrade path and NVRAM analysis on my Catalyst devices?
- Does the module firmware on my IPX/IGX/BPX devices need to be upgraded?

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To upgrade from Cisco.com:

Step 1 Select **Configuration > Tools > Software Image Management > Upgrade Analysis**.

The Select Upgrade Source dialog box appears.

Step 2 Select **Cisco.com** and click **Go**.

The Device Selection dialog box appears.

Step 3 Select the devices to analyze, then click **Next**.

See *Administration of Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

a. Enter your Cisco.com username and password.

If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

Admin > System > Cisco.com Settings > Proxy Server Setup

b. Click **OK** after entering the credential information.

The Cisco.com Upgrade Analysis dialog box appears with the following information:

Field	Description
Device	Name of the device
Running Image	Running image of the device

Field	Description
Image Options	Available images. Select the Image options from the drop-down list.
Error	Click on the link to review the details.

Step 4 Click **Finish** to update the upgrade path information.

The Upgrade Analysis Report appears in a new browser window.

See Understanding the Upgrade Analysis Report for details.

Planning an Upgrade From Repository

Use the Repository Upgrade Analysis option to analyze images in your software repository and determine the impact to and prerequisites for a new software deployment. The option produces the Upgrade Analysis report, which shows the required boot ROM, Flash memory, RAM, and access.

This option helps you answer such questions as:

- Does the device have sufficient RAM to hold the new software?
- Have the minimum ROM version requirements been met?
- Is the Flash memory large enough to hold the new software?
- Do I need to add Telnet access information for the device to the Device and Credential Repository?
- Does the module firmware on my IPX/IGX/BPX devices need to be upgraded?

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To upgrade from repository:

Step 1 Select **Configuration > Tools > Software Image Management > Upgrade Analysis**.

The Select Upgrade Source dialog box appears.

Step 2 Select **Repository**, then click **Go**.

The Repository Upgrade Analysis dialog box appears.

Step 3 From the list, select the image to analyze, then select the devices to upgrade, then click **Run Report**.

The Upgrade Analysis Report window appears.

See Understanding the Upgrade Analysis Report for details.

Understanding the Upgrade Analysis Report

The Upgrade Analysis report summarizes the impact to and prerequisites for a new software deployment for the selected devices. It is generated by the Cisco.com Upgrade Analysis (Planning an Upgrade From Cisco.com) and Repository Upgrade Analysis (Planning an Upgrade From Repository) options.

The information that is shown in this report depends on the device type you have selected. See these tables to understand the Upgrade Analysis Report, Table 8-5 and Table 8-6.

Locate your device in the Supported Image Import Features for Software Management table on Cisco.com. For some devices the upgrade analysis option may not be available yet.

http://www.cisco.com/en/US/partner/products/ps11200/products_device_support_tables_list.html

Table 8-5 Upgrade Analysis Report Columns

Column	Description
Device Information	Running Image Name, Running Image Version, BootROM Version, Running Image Feature, and Device Family
Boot ROM Upgrade	Any boot ROM upgrade required
Flash Upgrade	Any Flash upgrade required
RAM Upgrade	Any RAM upgrade required
Telnet Access	Any Telnet information required
Boot Flash Upgrade	Any boot Flash upgrade required
NVRAM Upgrade	Any NVRAM upgrade required
Module Firmware Upgrade	Firmware upgrade requirements for each service module in device.
Firmware Compatibility	Indicates whether the selected firmware image is compatible with the switch software image running on the device.

:The following table (Table 8-6) maps the Upgrade Analysis Report to the supported device types:

- Optical Networking
- Routers and Switches
- Storage Networking

The Upgrade Analysis from Cisco.com and Repository are not supported for these device types because the required information for the upgrade analysis is not provided by the device:

- Universal Gateways and Access Servers
- Content Networking
- DSL and Long Reach Ethernet (LRE)
- Optical Networking
- Security and VPN
- Broadband Cable
- Voice and Telephony
- Network Management
- Wireless
- Cisco Interfaces and Modules

Table 8-6 Upgrade Analysis Report Based on Device Type

Upgrade Analysis Report Columns	Device Type: Routers and Optical Networking	Device Type: Switches	Device Type: Storage Networking
Boot ROM Upgrade	Supported	Not supported	Not supported
Flash Upgrade	Supported	Not supported	Not supported
RAM Upgrade	Supported	Supported	Supported
Telnet Access	Supported	Not supported	Supported
Boot Flash Upgrade	Not supported	Supported	Not supported
NVRAM Upgrade	Not supported	Supported	Not supported
Module Firmware Upgrade	Supported. See the Supported Image Distribution Features for Software Management table on Cisco.com for the router's device list that supports Module Firmware Upgrade. http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html	Supported. This is applicable for the following devices: • IPX/IGX/BPX device switch • MGX system	Not supported
Firmware Compatibility	Not supported	Supported. This is applicable for the following devices: IPX/IGX/BPX device firmware	Not supported

In addition to this information, you can use the Go To drop-down list to navigate to particular device analysis report.

Button	Description
Export to File (Icon)	Exports the analysis report in CSV or PDF format.
Print (Icon)	Generates a format that can be printed.

Support for In Service Software Upgrade

LMS supports In Service Software Upgrade (ISSU) process. This process allows Cisco IOS software images to be updated without rebooting the device. This increases network availability and reduces downtime caused by planned software upgrades.

To perform the image upgrade using this ISSU process, the running image and the upgrade image must be ISSU capable and should be available in the flash memory.

The ISSU image upgrade process may fail if:

- The running or the upgrade image is not available in the flash memory
- The running image is deleted because of flash cleanup operation performed while the job is running.

ISSU support is available only for the following devices:

- Cisco Catalyst 6000 Series IOS Dual Chassis (VSS) Switches
- Cisco Catalyst 6000 Series Dual Supervisor Switches

ISSU process can be applied to the following distribution methods:

- By devices [Basic]
- By image
- Use remote staging

To perform this ISSU image upgrade process:

- Select **Reboot immediately after downloading** in the Job Schedule and Options page of the Device Distribution flow.
- You can also customize the configurations available in the Issuconf.properties file located at:
  - *NMSROOT*/MDC/tomcat/webapps/rme/WEB-INF/conf/swim (On Solaris and Soft Appliance)
  - *NMSROOT*\MDC\tomcat\webapps\rme\WEB-INF\conf\swim (On Windows)

  NMSROOT is the LMS install directory.

You can configure the following properties in the Issuconf.properties file:

Variable	Description
RBTConfig	Configure the rollback timer. By default, the value of this variable is set as NO. If you configure the value as **`Yes`**, then rollback will happen for the value set in the variable *RollBackTime*.
RollBackTime	Enter the rollback timer (value in minutes). By default, the rollback time is set as 45. To consider the value for rollback timer you must set the RBTConfig value as **`Yes`**.
IssuSupImgVer	The ISSU supported version of the running image. For ISSU upgrade support, the value for this variable must be an ISSU capable image version such as **`SXI`**. This value can either match the version of the running image completely, or partially. For example, 12.2(33)SXI, or SXI.

The running software image version in the device must match the version configured in the Issuconf.properties.

If the running image or the upgrade image is not an ISSU capable image, or the version of the image is wrongly configured for the variable “IssuSupImgVer” in the Issuconf.properties file, then ISSU upgrade process will not happen and LMS proceeds with the normal upgrade process.

For example, if the running image version is 12.2(33)SXI, which is ISSU capable, and the version entered for the variable “IssuSupImgVer” is 12.2(33)SXH, then ISSU upgrade will not happen and LMS proceeds with normal upgrade process.

To fix this issue, you must provide the proper version for the variable “IssuSupImgVer” that is ISSU capable. For example, 12.2(33)SXI, or SXI.

Software Distribution Methods

You can distribute images to the devices in your network, using any of these options:

- Distribute by Devices [Basic]:

  This option enables you to select devices and perform software image upgrades to those devices. Software Management checks the current image on the device and recommends a suitable image and the appropriate image storage for distribution.

  See Distributing by Devices [Basic]

- Distribute by Devices [Advanced]:

  This option enables you to enter the software image and storage media for the device that you want to upgrade.

  The selected image and storage media is validated and verified for dependencies and requirements based on the device information that you entered when you added devices to the Device Credentials Repository.

  See Distributing by Devices [Advanced]

- Distribute by Images:

  This option enables you to select a software image from the software image repository and use it to perform an image upgrade on suitable devices in your network. This option is useful when you have to distribute the same image to multiple devices.

  See Distributing by Images.

- Remote Staging and Distribution:

  This option enables you to select a software image, store it temporarily on a device and then use this stored image to upgrade suitable devices in your network. This option is helpful when the LMS server and the devices (including the remote stage device) are distributed across a WAN.

  See Remote Staging and Distribution.

You can run the device upgrades job sequentially or in parallel. After the devices upgrade, you can also specify the reboot order. You can specify these options in the Job Schedule and Options dialog box.

During the image upgrade, Software Management:

- Checks the amount of Flash memory on the device. If Flash memory needs to be erased before the new system image is loaded and erasing is allowed, it erases the Flash memory. Before erasing the Flash, a warning message appears `Flash memory will be erased`.
- Performs MD5 Checksum check of the image when it is downloaded from Cisco.com directly. It also performs image size check once the image is copied to a device, to check if there was any network transfer issue. These are the image consistency checks performed by Software Management.
- Provides a running log of the upgrade job.
- E-mails a report on the results to the specified addresses after completing the upgrade.
- Inserts boot commands to activate the upgraded image.
- Reboots the device if the Reboot Schedule option has been set to Reboot Immediately.
- RAM value is not checked. Hence, distribution proceeds without any errors even if the RAM value is unknown.
- Min.Flash is ignored, if Min.Flash is unknown.
- Image cannot be used for upgrade, if Flash size is unknown.

After you schedule an image upgrade, you can use Software Management Job Browser (**Configuration > Job Browsers > Software Image Management**) to review, retry, or cancel a job.

After a successful distribution job, Software Management triggers

- An inventory and a configuration collection.
- A Change Audit log. You can generate a Change Audit Standard Report in the Report Generator window (**Reports > Audit > Change Audit > Standard**).

This section contains:

- Planning the Upgrade
- Configuring Devices for Upgrades
- Scheduling the Upgrade
- Authorizing a Distribution Job
- Distributing by Devices [Basic]
- Distributing by Devices [Advanced]]
- Distributing by Images

Planning the Upgrade

Planning the upgrade typically involves these phases:

- Identifying Possible Changes
- Satisfying the Prerequisites
- Maintaining Your Software Image Repository
- Testing the New Images

Identifying Possible Changes

Identifying which devices at your site might require software upgrades consists of these phases:

- Determine whether an upgrade is required

  You can learn about new features or fixes in different ways.

  You use the Browse Bugs option (**Reports > Cisco.com > Bug Summary**) to summarize the software image bugs for the devices in your network.

  You can schedule a Browse Bugs job to run at regular intervals. This will help you determine any bugs related to current running images on the devices.

  If you find a bug in your software, call the Technical Assistance Center (TAC) to know the status of the bug.

  Your sales engineer or channel partner notifies you of new features that might be appropriate for your site.

  You check Cisco.com periodically to review new release notes, bug-fix documentation, and marketing bulletins.

- Retrieve information about the upgrade

  Go to Cisco.com to read the most recent product Release Notes or bug-fix documentation. This information will help you determine the software image version you need.

- Determine whether the upgrade is really necessary

  After you determine the version you need, you can list the current software version numbers for your managed devices.

  You can generate this using (**Reports > Inventory > Software**)

Satisfying the Prerequisites

Run Cisco.com Upgrade Analysis or Repository Upgrade Analysis to determine the prerequisites for a new software deployment. See Upgrade Analysis for further details.

In addition, you need to answer questions such as:

- Have you supplied the minimum requirements such as the minimum device configuration requirements for each device? See Meeting Minimum Device Requirements for further details.
- Is the device running from Flash (RFF)?
- Does the device have multiple Flash partitions?
- Does the Supervisor board require a new software image?
- Have you satisfied the additional requirements for the devices?

  See Configuring Devices for Upgrades for further details.

Maintaining Your Software Image Repository

- Use the Adding Images to the Repository > Network option to import running images from all Software Management-supported devices in your network into the repository.

  See Adding Images to the Software Repository From the Network for further details.

- Since you can download new images to a device without using Software Management, eventually the software image repository might not reflect the images that are running on your network devices.

  To keep the repository current:

  – Review all software images in the repository.

    See Software Repository for further details.

  – Schedule the Synchronization report to run periodically.

    See Scheduling a Synchronization Report for further details.

  – Retrieve additional images from Cisco.com, another device, or a file system on your server.

    See Adding Images to the Software Repository for further details.

- Download Cisco images from Cisco.com during a scheduled distribution job.

Testing the New Images

To confirm the stability of your network after upgrades, test the new software images before you perform a full-scale deployment.

You cannot roll back software upgrades for supervisor modules on Catalyst 5000 series switches. Therefore, test the new images for these devices thoroughly before deploying them on your network.

Configuring Devices for Upgrades

This section lists all the required tasks that have to be performed on Cisco devices. This section also captures the following information:

- Meeting Minimum Device Requirements
- Meeting Additional Device Requirements
- Additional SFB Checks
- Configuring Telnet and SSH Access
- Configuring SCP
- Configuring RCP
- Configuring TFTP
- Configuring HTTP
- Meeting Microcode and Modem Firmware Requirements

Meeting Minimum Device Requirements

Before you can upgrade software images, you must meet the following requirements:

Category	Requirements
Device configuration	Device must be configured with SNMP read-write community string. There should not be any access list on the device that will disable TFTP transfers from the workstation.
IOS and ONS devices	For the device to be rebooted using the SNMP protocol, you must configure the **`snmp-server system-shutdown`** command on the device.
SFB devices	See Additional SFB Checks for further details.
RSP 7000 or 7500 devices running Cisco IOS version 11.x or later	See Additional SFB Checks for further details.
Microcode images	See Meeting Microcode and Modem Firmware Requirements for further details.
Inventory	SNMP read-write community string must be in Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices).
tftpboot directory space	Must have enough space for all concurrent jobs, which could include image distribution, image import, config file scan, and so on.

Meeting Additional Device Requirements

Before you upgrade, you must meet the following additional device requirements:

- Make sure you have Telnet access to upgrade the devices. Before you upgrade, add the Enable mode password (see Configuring Telnet and SSH Access) and access information for each device to the Device and Credential Repository.

  See the Software Management Functional Supported Device tables on Cisco.com for the devices list that requires Telnet access.

  http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html
- To perform the upgrade, the device must be rebooted to RxBoot mode using SNMP. Do this even if you have selected the Do not reboot option when scheduling the upgrade. This procedure is applicable only to RFF devices.
- Configure PIX Firewall for SNMP and telnet access. For LMS to manage these devices, you must enter these commands on the device, in the config mode:
  1. **`config terminal`**
  2. **`snmp -server host`** *hostname*
  3. **`snmp -server community`** *community name*
  4. **`telnet`** *ip* 255.255.253.255 *inside interface*
  5. **`write mem`**

Additional SFB Checks

Software Management validates the image upgrades at the time the job is scheduled. For SFB devices, Software Management also verifies that:

- IP routing is enabled on the device.
- The ethernet interface that connects LMS to the device has an IP address assigned to it and is routing IP protocol.
- If the device is configured with Frame Relay subinterfaces, the device software version is 11.1 or higher.
- The ROM monitor code version is 5.2 or higher.

Configuring Telnet and SSH Access

Before you schedule the upgrade, use the Device and Credentials (**Inventory > Device Administration > Add / Import / Manage Devices**) option to add or change passwords and access information.

When you select the SSH protocol for the Software Management, the underlying transport mechanism checks whether the device is running SSHv2.

If so, it tries to connect to the device using SSHv2.

If the device does not run SSHv2 and runs only SSHv1 then it connects to the device through SSHv1.

If the device runs both SSHv2 and SSHv1, then it connects to the device using SSHv2.

If a problem occurs while connecting to the device using SSHv2, then it does not fall back to SSHv1 for the device that is being accessed.

See the Software Management Functional Supported Device tables on Cisco.com for the devices list that requires Telnet and SSH access.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

- Telnet password

  If the Telnet password is configured on your device, you might need this password for basic login access.

  Enter the Telnet password in the *Primary Credential Password* field in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- Local user name

  If the device is configured with the local username and password, you must enter this information when you log in. In Telnet mode, for catalyst devices, the local user name is not applicable, so you must leave this field blank. In secure shell (SSH) mode, for catalyst devices, you must enter this information.

  Enter the Local User name in the *Primary Credential Username* field in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- Local user password

  If the device is configured with the local username and password, you must enter this information when you log in.

  If TACACS is configured, the application uses the TACACS information.

  If the parent TACACS server is down and the local username and password are present, the application uses this information instead.

  Enter the Local user password in the *Primary Credential Password* field in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- TACACS username and password

  If the device is configured for TACACS, you must enter the TACACS username and password. The application will try to use this information first for login access.

  Enter the TACACS username and password in the *Primary Credential Username* and *Primary Credential Password* fields in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- Enable secret password

  The enable secret password takes precedence over the enable password in Cisco IOS Release 11.x and later. Use this password to make changes when running in regular Cisco IOS mode. If the service password-encryption is enabled, enable secret passwords are more secure than enable passwords.

  Enter the Enable password in the *Primary Credential Enable Password* field in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- Enable password

  Since some versions of BOOT ROM mode do not recognize the enable secret password or if enable secret is not configured on the device, you must use the enable password to load Flash memory.

  Enter the Enable password in the *Primary Credential Enable Password* field in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- Enable TACACS

  Sometimes the device is configured for enable TACACS. In this case, you must provide the TACACS user name and password information for enable access.

Note The TACACS user name and password must be same as the Local user name and password. You cannot configure different user names and passwords for user mode and enable mode for the device.

Some useful URLs on configuring SSHv2 are:

- Configuring Secure Shell on Routers and Switches Running Cisco IOS:

  http://www.cisco.com/warp/public/707/ssh.shtml

- How to Configure SSH on Catalyst Switches Running Catalyst OS:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a0080094314.shtml

- Configuring the Secure Shell Daemon Protocol on CSS:

  http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/css11500series/v8.20/configuration/security/guide/sshd.html

- Configuration Examples and TechNotes:
  - http://www.cisco.com/en/US/tech/tk583/tk617/tech_configuration_examples_list.html

Configuring SCP

You can use the SCP protocol to transfer the software images. While using SCP protocol, the LMS server acts like a client and the device acts like a server.

To configure the LMS server as an SCP client, you must enter the SSH credentials. See Configuring Telnet and SSH Access for further details.

For Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches, if you are upgrading the .tar images using SCP protocol, you must configure the SCP username and password.

The minimum supported version of the running image should be 12.2(25) SEC and should have the SCP protocol support.

In this case, LMS server acts like a SCP server and the device acts like a client.

To configure SCP username and password:

Step 1 Go to **Admin > System > System Preferences**.

The System Preferences dialog box appears.

Step 2 Enter the following information:

Field	Description
SCP User	Enter the user name. For Solaris and Soft Appliance: • You must specify a user name that has SSH authorization. SCP uses this authorization for transferring the images. For Windows: • The username you have entered here is taken for transferring images using SCP protocol.
SCP Password	Enter the password. For Solaris and Soft Appliance: • You must specify a password that has SSH authentication. SCP uses this authentication for transferring the images. For Windows: • The password you have entered here is used for authentication while transferring images using SCP protocol.
SCP Verify Password	Re-enter the password to verify.

Step 3 Click **Apply** after making the changes.

Step 4 To cancel the changes, click **Cancel**.

Configuring RCP

You can use the RCP protocol to transfer the software images. The LMS server acts like a RCP server and the device acts like a client.

Configuring RCP involves the following:

- Configuring RCP on Solaris and Soft Appliance
- Configuring RCP on Windows
- Selecting RCP as the Active File Transfer Method on Solaris and Soft Appliance and Windows
- Configuring Cisco IOS Software Devices to Allow RCP Transactions

Configuring RCP on Solaris and Soft Appliance

Configuring RCP on Solaris and Soft Appliance, involves the following:

- Creating the RCP Remote User Account
- Enabling the RCP Daemon

Creating the RCP Remote User Account

To use RCP, you must create a user account on the system to act as the remote user to authenticate the RCP commands issued by devices. This user account must own an empty.rhosts file in its home directory to which the user, casuser has write access.

You can choose the name of this user account because you can configure the LMS server to use any user account.

The default user account name is *cwuser*. The examples in this procedure use the default name *cwuser*. If you choose to use a different name, substitute that name for *cwuser*.

To create and configure the RCP remote user account, follow these steps while logged in as root:

Step 1 To add a user account named cwuser to the system, enter:

```
# useradd -m -c "user account to authenticate remote copy operations" \ cwuser
```

Step 2 Navigate to the *cwuser* home directory.

Step 3 Create the .rhosts file, by entering:

```
# touch .rhosts
```

Step 4 Change the owner of the .rhosts file, by entering:

```
# chown cwuser:casusers .rhosts
```

Step 5 Change the permissions of the .rhosts file, by entering:

```
# chmod 0664 .rhosts
```

If you did not use the default user name *cwuser*, use the user account that you created as the RCP remote user account.

a. Login to the server as admin.

b. Select **Admin > System > System Preferences**.

The View / Edit System Preferences dialog box appears.

c. Enter the name of the user account that you created in the RCP User field, then click **Apply**.

Enabling the RCP Daemon

To add and configure standard Solaris and Soft Appliance RCP server software:

Step 1 Log in as superuser.

Step 2 Edit the /etc/inetd.conf file using a text editor.

- Look in the file /etc/inetd.conf for the line that invokes rshd. If the line begins with a pound sign (#), remove the pound sign with a text editor. Depending on your system, the line that invokes the rshd server might look similar to:

```
shell   stream  tcp    nowait  root    /usr/sbin/in.rshd   in.rshd
```

- Save the changes to the edited file and exit the text editor.

Step 3 Go to the UNIX prompt, enter the following to display the process identification number for the *inetd* configuration:

```
# /usr/bin/ps -ef | grep -v grep | grep inetd
```

The system response is similar to:

```
root  119   1  0  12:56:14 ?           0:00 /usr/bin/inetd -s
```

The first number in the output (119) is the process identification number of the *inetd* configuration.

Step 4 Enable your system to read the edited /etc/inetd.conf file, enter:

 # kill -HUP *119*

where *119* is the process identification number identified in Step 3.

Step 5 Verify that rshd is enabled by entering:

 # netstat -a | **grep shell**

which should return output similar to:

```
*.shell    *.*     0 0 0 0 LISTEN
```

Configuring RCP on Windows

During LMS installation, the RCP server is configured.

Selecting RCP as the Active File Transfer Method on Solaris and Soft Appliance and Windows

Step 1 Select **Admin > Network > Software Image Management > View/Edit Preferences**.

The View/Edit Preferences dialog box appears.

Step 2 Select the **Protocol Order**.

Step 3 Click **Apply**.

Configuring Cisco IOS Software Devices to Allow RCP Transactions

Given here is a basic configuration in a router that can handle RCP transactions from the LMS server.

```
calvi# show running configuration
Building configuration...

Current configuration:
!
version 11.3 service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname calvi
!
boot system c2500-is-l.113-11a.T1.bin 255.255.255.255
enable password 7 1106170043130700
!
username cwuser password 7 000C1C0A05
ip rcmd rcp-enable
ip rcmd remote-host cwuser 172.17.246.221 cwuser enable
ip rcmd remote-username cwuser
```

```
!
!
process-max-time 200
!
interface Loopback0
 ip address 5.5.5.5 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0
 description Connection to Backbone
 ip address 172.17.246.4 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 no ip address
 no ip mroute-cache shutdown
 no cdp enable

!
interface Serial1
 no ip address
 no ip mroute-cache shutdown
 no cdp enable
!
interface Async1
 no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.246.1
!
logging monitor informational
snmp-server community private RW
snmp-server community public RO
snmp-server enable traps snmp
snmp-server host 172.17.246.117 traps public

!
line con 0
 exec-timeout 0 0
 password 7 0504080A754D4205
 login
line 1 8
 exec-timeout 0 0
 login
 transport input all
line aux 0
```

```
 password 7 06090124184F0515
 login
line vty 0 4
 exec-timeout 0 0
 password 7 06090124184F0515
 login
!
end
```

where:

- `username cwuser password 7 000C1C0A05` creates the username cwuser on the router. You must choose a password for this user.
- `ip rcmd rcp-enable` enables RCP service on the device.
- `ip remote-host cwuser 172.17.246.221 cwuser enable` The remote system where you install LMS has the IP address 172.17.246.221 and the local definition of the user, cwuser. This command allows cwuser to issue the copy command on the network device.
- `ip rcmd remote-username cwuser` configures use of the remote user name at the request of a remote copy. At the initiation of the remote copy operation in the network device, for example, in Add Images to Library, the device uses the cwuser name to authenticate against the LMS server.

Configuring TFTP

You can use the Trivial File Transfer Protocol (TFTP) protocol to transfer the software images. The LMS server acts like a TFTP server and the device acts like a client.

Configuring TFTP on Windows

During LMS installation, the tftpboot directory is created under the directory in which LMS is installed (the default is *SystemDrive*:\Program Files\CSCOpx).

Configuring TFTP on Solaris and Soft Appliance

A file transfer server must be installed on your system. You must enable a TFTP server because it is the default file transfer server type.

During Software Management installation, if the installation tool cannot find a TFTP server, it tries to add one. If the installation tool cannot find or create a TFTP server, you must install and enable the TFTP server. Verify that a /tftpboot directory exists, as explained in the following sections.

- Enabling the TFTP Daemon
- Creating the /tftpboot Directory

Enabling the TFTP Daemon

If you are using standard Solaris and Soft Appliance software, you can add and configure the TFTP server (TFTPD).

Step 1 Log in as superuser.

Step 2 Edit the /etc/inetd.conf file using a text editor.

- Look in the file /etc/inetd.conf for the line that invokes TFTPD. If the line begins with a pound sign (#), remove the pound sign with your text editor. Depending on your system, the line that invokes the TFTP server might look similar to:

  ```
  tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
  ```

- Save the changes to the edited file and exit your text editor.

Step 3 Go to the UNIX prompt, enter the following command to display the process identification number for the inetd configuration:

```
# /usr/bin/ps -ef | grep -v grep | grep inetd
```

The system response is similar to:

```
root  119   1  0  12:56:14 ?           0:00 /usr/bin/inetd -s
```

The first number in the output (119) is the process identification number of the inetd configuration.

Step 4 Enable your system to read the edited /etc/inetd.conf file, enter:

`# kill -HUP` *119*

where *119* is the process identification number identified in Step 3.

Step 5 Verify that TFTP is enabled by entering either:

```
# netstat -a
```

or

```
# grep tftp
```

which should return output similar to:

```
*.tftp Idle
```

or enter:

`# /opt/CSCOpx/bin/mping -s tftp` *localhost_machine_name*

which returns the number of modules sent and received, for example:

```
sent:5 recvd:5 . ..
```

If the output shows that zero modules were received, TFTP is not enabled. Repeat these steps, beginning with Step 1, to make sure you have enabled TFTP.

Creating the /tftpboot Directory

LMS uses the /tftpboot directory when transferring files between the LMS server and network devices. The files are removed after the transfer is complete. However, multiple jobs (for example, image distribution, image import, or config file scan) could be running at the same time.

Each of these jobs requires its own space. Software image sizes, for example, can be up to 20 MB. To ensure that jobs run successfully, make sure there is sufficient space available in the /tftpboot directory.

If the /tftpboot directory does not exist on your system, you must create it:

Step 1 Enter:

```
# mkdir /tftpboot
```

Step 2 Make sure all users have read, write, and execute permissions to the /tftpboot directory by entering:

```
# chmod 777 /tftpboot
```

The /tftpboot directory now exists and has the correct permissions.

Configuring HTTP

No configuration on device is required for this protocol.

Meeting Microcode and Modem Firmware Requirements

The following minimum system software versions are required to support microcode and modem firmware upgrades. However, different versions of these image types might require different versions of system software.

Software Management does not check for compatibility and dependence between each microcode version and system software version. It merely warns the user to check this information by consulting a technical representative or the compatibility matrix published on Cisco.com.

MICA Portware Image Types

Device	Minimum System Software Version
AS5200	Cisco IOS version 11.3(2)T Bootloader version 11.2(11)P
AS5300	Cisco IOS version 11.2(9)XA
3640	Cisco IOS version 11.2(12)P

Microcom Firmware Image Types

Device	Minimum System Software Version
AS5200	Cisco IOS version 11.2(10a)P Bootloader version 11.2(11)P
AS5300	Cisco IOS version 11.1(14)AA

CIP Microcode Image Types

Supported for Cisco IOS versions 11.x and later.

Scheduling the Upgrade

Scheduling an upgrade consists of:

- Selecting the devices to upgrade

  Use Software Management's scheduling features to schedule the upgrade for one device or a series of devices.

  Software Management downloads images from more than one device in parallel. You must ensure that the tftpboot directory (*NMSROOT*/tftpboot (On Solaris and Soft Appliance), and *NMSROOT*\tftpboot (On Windows)) has enough free space to accommodate at least 20 images.

- Determining any limitations or requirements for the selected devices

  For example, SFB devices have several upgrade requirements and limitations.

- Updating the inventory

  Since Software Management uses the inventory to make image and Flash memory recommendations, be sure that your current inventory reflects the correct device information.

  For some devices such as 6400 NRP1, 801, and 802, etc., Software Management contacts devices to get the Flash information.

- Configuring file transfer protocol order

  Before scheduling a software upgrade job, set the protocol order for configuration file transfer.

  For fetching configuration from device, the protocol settings of Configuration Management are used. Software Management uses the same protocol for fetch and download of configurations. You can set the Configuration Management protocol order using **Admin > Collection Settings > Config > Config Collection Settings**.

  For better performance, set *tftp* as the first protocol.

- Determining the upgrade and execution order

  Based on your network topology and to minimize the impact on your network, you can schedule the upgrades job either sequentially or in parallel.

  For example, if devices A, B, and C are networked sequentially, then you must upgrade device C first, then device B, then device A. If you upgrade device B first, you might no longer have access to device C.

- Determining the upgrade schedule

  For most devices, you can schedule the software to:

  – Distribute the software to the device and reload the device immediately.

  – Distribute the software only. You will perform the reloads manually.

  The following devices are always rebooted immediately after the software is downloaded:

  – Single Flash bank devices

  – FDDI/CDDI, ATM, and Token Ring modules on Catalyst switches

- Checking the Work Order report

  The Work Order report contains such information as the state of the software running on the device and the new software, the operations that will be performed during the upgrade procedure, and any important notes that you should be aware of before the upgrade begins.

Authorizing a Distribution Job

The Job Approval approval option allows you to require job upgrade approvals before running a scheduled job. It enforces the approval process by sending job requests through e-mail to people on the approver list.

To set up the authorization process:

- Select the appropriate Job Approval options.
- Make sure one or more approver lists exist.
- Make sure the upgrade job identifies an approver list.
- Make sure the approver is a member of that approver list.

See *Administration of Cisco Prime LAN Management Solution 4.1* for more details on creating and editing approver lists, assigning approver lists, setting up Job Approval, and approving and rejecting jobs.

Distributing by Devices [Basic]

You can use the Distribute by Devices option to schedule device-centric upgrade jobs.

Software Management recommends any software images available on LMS server and Cisco.com, if this option is selected by you (**Admin > Network > Software Image Management > View/Edit Preferences**).

To do this, select the devices first and distribute suitable images to them. After the distribution job is complete, you can use the Software Management Job Browser window to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.

  You can also download the images from Cisco.com. You must ensure that you have the access to download the images from Cisco.com.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the images by device in Basic mode:

Step 1 Select **Configuration > Tools > Software Image Management > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **By device [Basic]** and click **Go**. The Select Devices dialog box appears.

Step 3 Select the devices, then click **Next**.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

a. Enter your Cisco.com username and password.

If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

Admin > System > Cisco.com Settings > Proxy Server Setup

- Click **OK** after entering the credential information.

The software management analyzes the required images that are available in your software repository and on Cisco.com. It then recommends the appropriate image for distribution.

See Understanding Upgrade Recommendations for details on how Software Management recommends image for various Cisco device types.

The Distribute By Devices dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Image Options	Details of the recommended image.
Storage Options	Details of recommended image storage information.
Errors	Click on the underlined Error message to review the details.

Notation Descriptions

- An asterisk (*) at the beginning of the field indicates the recommended image or partition by Software Management. If there is no asterisk at the beginning of the field, it indicates that an appropriate image or partition could not be found but the displayed selections might work.
- A '^' means that the image resides in Cisco.com but not in your software image repository. When you select an image in Cisco.com to distribute to a network device, the image is first added to the image repository, then downloaded to the device.
- A superscript '1' refers to read-only Flash memory.
- A superscript '2' refers to the Flash partition that holds the running image when a device is running from Flash (RFF).

Step 4 Select the devices to which you want to distribute images and click **Next**.

The Distribute By Devices window appears with these details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Image	Image information that you have selected.

Field	Description
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Step 5 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule the job.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Comments	Enter additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).

Field	Description
Perform distribution in Non-Installed mode	This option is available only if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If the running image is in the repository, select this option to place a copy in the TFTP server directory. Uses this copy of image if reboot with new image fails. Note the following about this option: • Option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in TFTP server directory so that the device can find it any time it reboots
Backup current running image	Select to back up the running image in software image repository before upgrading. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do *not* select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (**Inventory > Device Administration > Add / Import / Manage Devices**) are ignored.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your device list. 3. Click **Done**.

Field	Description
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click **Done**.

Step 7 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verification warnings generated during image distribution (if applicable).

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Distributing by Devices [Advanced]

You can use the Distribute by Devices option to schedule device-centric upgrade jobs.

The selected image and storage media is validated and verified for dependencies and requirements based on the device information that you have provided at the time of adding devices to the Device and Credential Repository and the device data that is collected by the inventory.

The images that you want to distribute must be available in the Software repository.

You can use this method to upgrade the System software on all Software Management supported devices. You can also upgrade module software on those modules which have a management IP address.

The modules/interfaces that do not have a management IP address cannot be upgraded using this method.

The input file that contains the details of the device and image must be available at this location:

On Solaris and Soft Appliance:

/var/adm/CSCOpx/files/rme/swim/advdistinput

On Windows:

NMSROOT\files\rme\swim\advdistinput

Where *NMSROOT* is the LMS installed directory.

After the distribution job is complete, you can use the Software Management Job Browser window to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device. You should have verified whether the necessary software images are present in the image repository.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the images by device in Advance mode:

Step 1 Select **Configuration > Tools > Software Image Management > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **By device [Advanced]**, then click **Go**.

The Expert Distribution dialog box appears.

Step 3 Click **Browse**.

The Server Side File Browser dialog box appears.

Step 4 Select the file and click **OK**.

The input file that contains the details must be available at this location:

On Solaris and Soft Appliance:

/var/adm/CSCOpx/files/rme/swim/advdistinput

On Windows:

NMSROOT\files\rme\swim\advdistinput

Where *NMSROOT* is the LMS installed directory.

The selected file must contain the information in CSV format and all the fields are mandatory:

device-display-name,image-in-repository,storagedestination,moduleidentifier

- *device-display-name*—Name of the device as entered in Device and Credential Repository.
- *image-in-repository*—Image name as in the software image repository.

- *storagedestination*—Image storage destination
- *moduleidentifier*—Module identifier number. This is applicable only for Catalyst devices. For other devices, you must enter 0.

  You can identify the device module number using Inventory Detailed Device Report (**Reports** > **Inventory** > **Detailed Device**). In the Detailed Device Report, the *Slot Number* column in the *Module Information* table provides you the Module Identifier Number.

For example, for a Cisco Router:

```
Rtr1750,c1700-sy56i-mz.121-24.bin,flash:1,0
```

For a Cisco Catalyst device:

```
cat5500-10.100.38.17,cat5000-supg.6-4-10.bin,bootflash:,1
```

Step 5 Do either of the following:

- Check the Skip Verification checkbox if you want to postpone the verification to the job execution stage.

  If you have checked the Skip Verification checkbox, go to Step 7.

Or

- Click **Verify** if you want the verification to take place during the job scheduling stage itself.

  If you have clicked **Verify**, go to Step 6.

Step 6 When you click Verify, the Expert Distribution window is updated with the following device details:

Field	Description
Device	Name of the device as specified in the input file.
Image	Name of the image as specified in the input file.
Storage Destination	Image storage information as specified in the input file.
Module Number	Module identifier number as specified in the input file.
Result	Click on the link to review the details.

Step 7 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 8 Enter the following information in the Job Schedule and Options dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (by device [Advanced]) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule the job.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Comments	Enter additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Applies to Supervisor Engine I, II, and III only. Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is available only if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated. • Applies to Supervisor Engine III only.
Use current running image as tftp fallback image	If the running image is in the repository, select this option to place a copy in the TFTP server directory. Uses this copy of image if reboot with new image fails. Note the following about this option: • Applies to Supervisor Engine I, II, and III only. • Option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in TFTP server directory so that the device can find it any time it reboots

Field	Description
Back up current running image	Select to back up the running image in software image repository before upgrading. Applies to Supervisor Engine I, II, and III only. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do *not* select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	Enter the password for the distribution job. This password is used to Telnet to the devices at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (**Inventory > Device Administration > Add / Import / Manage Devices**) are ignored.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click **Done**.

Step 9 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)

- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verification warnings generated during image distribution (if applicable).

Step 10 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Distributing by Images

You can use the Distribute by Images option to schedule image-centric upgrade jobs. To do this, you must first select an image and then distribute it to applicable devices.

After the distribution job is complete, you can use the Job Details report to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

You cannot use this procedure to upgrade:

- MICA portware
- Microcom firmware
- CIP microcode
- Bootloader for IOS
- Catalyst modules other than the Supervisor module

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device. You should have verified whether the necessary software images are in the image repository.

  See Planning the Upgrade for further details.
- Considered the effect of the upgrade on your network and your network users.

  See Scheduling the Upgrade for further details.
- Supplied the information required by Software Management for each device.

  See Configuring Devices for Upgrades for further details.

To distribute images by image:

Step 1 Select **Configuration > Tools > Software Image Management > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **By image**, then click **Go**.

The Select Image And Devices dialog box appears.

Step 3 Select:

a. An image from the software image repository.

b. Devices that need upgrading

Step 4 Click **Next**.

The Device Recommendation dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Recommended Storage	Details of recommended image storage information.
Error	Click on the link to review the details.

Notation Descriptions

- An asterisk (*) at the beginning of the field indicates the recommended partition by Software Management. If there is no asterisk at the beginning of the field indicates, an appropriate partition could not be found but the displayed selections might work.
- A superscript '1' refers to read-only Flash memory.

Step 5 Select the devices you want to upgrade, then click **Next**.

The Image Centric Distribution Verification window appears. This window displays the following information:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Software management recommends the Flash partition with the maximum free space in each device. You can override the recommendation and select another partition from the drop-down box.

Step 6 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 7 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (by image) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule the job.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following: • This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots
Back up current running image	Select to back up running image in software image repository before upgrading. Line cards do not support upload.

Field	Description
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do *not* select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (**Inventory > Device Administration > Add / Import / Manage Devices**) are ignored.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click **Done**.

Step 8 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.

- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verification warnings generated during image distribution (if applicable).

Step 9 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your job, select **Configuration > Tools > Software Image Management > Jobs**.

Support for IOS Software Modularity

Software Management provides support for Cisco IOS Software Modularity Images. The Cisco IOS Software Modularity Images combine subsystems into individual processes and enhances the memory architecture in order to provide the process level fault isolation and subsystem In-Service Software Upgrade (ISSU) capability.

Traditionally, IOS Software images are distributed by:

- Copying the image to disk.
- Updating boot commands and rebooted.

The IOS Software Modularity images can be run in this mode as well. This is called Cisco IOS Software Modular non-install mode (also known as binary mode).

Software Management supports distribution of Patches and Maintenance Packs. This distribution is accomplished by the use of Cisco IOS Software Modularity Images. Software Modularity enhances the IOS infrastructure to allow selective system maintenance through individual patch upgrades. See Patch Distribution for more details.

Patches

A patch is a single fix that may affect one or more subsystems. Patches can only be installed to a search root, where a base image exists. Patches are released for a particular base image version and device platform.

Maintenance Pack

A Maintenance Pack includes one or more patches. This pack is applied like a Patch. Maintenance Packs are released for a particular base image version and device platform.

Note Software Management does not support downloading Patches/Maintenance Packs from Cisco.com. The reason is that these images are available in an external URL. You have to manually download patches from the external URL and add the same to Software Repository.

Modes of Distribution

There are two modes of distribution of Software Modularity images to devices:

- Non Installed Mode

  This process involves the distribution of images by copying of the IOS Software Modularity images to the hard disk of the device, updating the boot commands and rebooting the OS on the device. You can run the Cisco IOS Software Modularity Images in this mode and so it is also called IOS Software Modularity non-install mode. It is also known as binary mode.

- Installed Mode

  According to this mode the IOS Software Modularity image is extracted/uncompressed to a compact Flash with a well defined directory structure. The installed mode provides the advantage of accomodating the point fix capabilities of Software Modularity.

Note Software Management checks the current image on the device and recommends a suitable image and the appropriate image storage for distribution. Software Management only recommends Maintenance Pack Images for devices. It does not recommend patches for devices.

Cisco IOS Software Modularity base images support:

- Import of Image from Cisco.com
- Import of Image from device
- Import of Image form File System
- Import of Image from Network
- Cisco.comUpgrade Analysis
- Distribution of Images
- Software Repository Synchronization

Support for Import of Image from device, Import of Image from Network and Software Repository Synchronization is applicable only for devices running IOS Software Modularity images in non-installed mode.

The population of Flash files on Cisco-Flash-MIB is not done on the devices running IOS Software Modularity image versions 12.2(18)SXF4 and 12.2(18)SXF5 and so these image versions are not supported by Software Management. The minimum IOS Software Modularity image version supported by Software Management is 12.2(18)SXF6.

Patch Distribution

You can distribute patches simultaneously to applicable devices. Patch distribution does not require reboot of the entire OS on a device. You can install a patches only to a search root where a base image exists. Patches, once installed, must be activated to come to effect on the running system.

Note You can apply Patches or Maintenance Packs to a device only if the device is running IOS Software Modularity Images in installed mode.

Software Management verifies:

- Patches against the base image and device platform to ensure compatibility. If the patches are incompatible then those patches are rejected.
- Whether the target patch already exists on the device.

Patch Distribution Methods

You can distribute patch images to the devices in your network, using any of these methods:

- Distribute by Devices

  This method enables you to select devices and perform patch upgrades to those devices.

  See Patch Distribution - by Devices.

- Distribute by Patch

  This method enables you to select a patch image from the Software Repository and use it to perform a patch upgrade on suitable devices in your network. This option is useful when you have to distribute the same patch image to multiple devices.

  See Patch Distribution - by Patch.

Patch Distribution - by Devices

You can use the Distribute by Devices option to schedule device-centric patch upgrade jobs.

Software Management recommends any Maintenance Pack software images available in the Repository.

Note Currently Software Management does not support importing of patch images from Cisco.com. You need to import patch images into local filesystem and then import into repository by using Import from file system. See Adding Images to the Software Repository From a File System for more details.

Before You Begin

Before you begin distributing the patch images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the patch images by device:

Step 1 Select **Configuration > Tools > Software Image Management > Patch Distribution**.

The Patch Distribution Method dialog box appears.

Step 2 Select **By devices** and click **Proceed**.

The Patch Distribute by Devices dialog box appears. The Device Selector lists all the available devices.

Step 3 Select the devices, then click **Next**.

If any of the selected device is not in install mode, an error message is displayed:

```
Device is not in installed mode or not patchable
```

Unselect the device that is not in installed mode and continue.

The software management analyzes the required patch images that are available in your software repository and lists the applicable patch images for each device selected. You can select one or more required patches from the list for each device by using the Ctrl key.

You should select at least one patch for each selected device. If you do not select a patch for a device, an error message is displayed.

```
You should select atleast one patch image for each selected device.
```

Ensure that you select at least one patch for each selected device and continue.

The Patch Distribute By Devices dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Patch type, chassis model, and software version on device.
Patches Options	Details of the patch.
Storage Location	Details of the storage location of the selected patch image.
Errors	Click on the underlined Error message to review the details.

Step 4 Select the devices as well as the patch images you wish to distribute to the selected devices and click **Next**.

The Patch Distribute By Devices window appears with these details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Patch	Patch information that you have selected.
Selected Slot	Image storage information from where the current base image is running.
Verification Result	Click on the link to review the details.

Step 5 Click **Next**. The Job Schedule and Options dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Patch Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule the job.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter additional information about this job.
Job Options	
Activate Patches	Select if you want to activate the patches immediately after download.
Reboot if it needs.	Select if the patch activation requires a reboot. Unselect if the patch activation does not require a reboot.
On error, stop processing subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do *not* select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	This option is checked, when the user name, password and enable password are provided for the job.
User Name	Enter the username for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Password	Enter the password for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Enable Password	Re-enter the password for confirmation purpose.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.

Field	Description
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click **Done**.

Step 7 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Patches selected for the upgrade.
- Job Approval information.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verify warnings generated during patch distribution (if applicable).

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Patch Distribution - by Patch

You can use the Distribute by Patch option to schedule patch upgrade jobs.

Note Currently Software Management does not support importing of patch images from Cisco.com. You need to import patch images into local filesystem and then import into repository by using Import from file system. See Adding Images to the Software Repository From a File System for more details.

Before You Begin

Before you begin distributing the patch images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.

- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the patch images by device:

Step 1 Select **Configuration > Tools > Software Image Management > Patch Distribution**.

The Patch Distribution Method dialog box appears.

Step 2 Select **By Patch** and click **Proceed**.

The Distribute by Patch dialog box appears.

Step 3 Select a patch from the Image Selection pane and devices from the Device Selection pane, and click **Next**.

The Distribute By Patch - Recommendations dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of the storage location of the selected patch image.
Errors	Click on the underlined Error message to review the details.

Step 4 Select the devices as well as the patch images you wish to distribute to the selected devices and click **Next**.

The Distribute By Patch - Verification window appears with these details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information from where the current base image is running.
Verification Result	Click on the link to review the details.

Step 5 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Patch Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule the job.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter the additional information about this job.
Job Options	
Activate Patches	Select if you want to activate the patches immediately after download.
Reboot if it needs	Select if the patch activation requires a reboot. Unselect if the patch activation does not require a reboot.
On error, stop processing subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do *not* select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	This option is checked, when the user name, password and enable password are provided for the job.
User Name	Enter the username for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Password	Enter the password for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Enable Password	Re-enter the password for confirmation purpose.

Field	Description
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click **Done**.

Step 7 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Patches selected for the upgrade.
- Job Approval information.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verify warnings generated during patch distribution (if applicable).

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Remote Staging and Distribution

The Remote Staging and Distribution option helps you to upgrade multiple devices over a WAN.

You can perform remote staging and distribution by any one of the methods:

- External FTP server
- External TFTP server
- Remote Staging Device

In this workflow, a managed device or external TFTP server or FTP server is used to stage an image temporarily. The staged image is then used to upgrade devices that are connected by LAN to the Remote Stage device or external TFTP server or FTP server. If you use this method, you do not have to copy a similar image, multiple times across the WAN.

After the image distribution job is completed using a managed device as a remote stage device, the configuration changes made to the Remote Stage device are automatically reversed and the staged image is deleted from the Remote Stage device.

After the distribution job is complete, you can use the Software Image Management Job Browser to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

This section contains:

- Using External FTP Server
- Using External TFTP Server
- Using Remote Stage Device

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Supported Remote Stage Devices

The device that is used as the Remote Stage must have enough free Flash space to copy the selected image.

See the Supported Image Distribution Features for Software Management table on Cisco.com for Remote Staging devices list.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

Before You Begin

Before you begin distributing the images, you should:

- Prepare for this upgrade. You should have met all of the prerequisites for loading the software on the device or external TFTP server or FTP server. You should also verified whether the necessary software images are in the image repository.
- Manually copy the software image to the External TFTP server or FTP server. This is if you are using the External TFTP/FTP server as the Staging Server.
- Consider the effect of the upgrade on your network and your network users.
- Supply the necessary information required by Software Management for each device.

- Decide on the device or external TFTP server or FTP server that you will use as the Remote Stage device or server.
- Ensure that the Telnet or SSH protocols are functioning properly if you are planning to distribute the images to devices using a External FTP server. The connection protocol for running FTP commands on the device can be either Telnet or SSH.

Note For the devices that supports remote staging using external FTP Server, see Supported Devices for FTP.

To distribute images using Remote Staging:

Step 1 Select **Configuration > Tools > Software Image Management > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **Use remote staging** and click **Go**.

The Remote Staging and Distribution dialog box appears.

Step 3 Select any of the following:

- **Using External FTP Server** to use an external FTP server as the staging server.

  For more information, see Using External FTP Server.
- **Using External TFTP Server** to use an external TFTP server as the staging server.

  For more information, see Using External TFTP Server.
- **Using Remote Stage Device** to use a device as the remote staging device.

  For more information, see Using Remote Stage Device.

Using External FTP Server

LMS Software Management uses the External FTP server option to upgrade software images in one or more devices. When you select this option, you must enter the FTP credentials and image location.

The FTP copy command is arrived at based on the FTP credentials that you enter. Software Management uses Telnet or SSH protocol to connect to the devices and deploy the FTP `copy` command. This command gets the software images from the specified location in the FTP server.

Only WLSE and NAM devices support image distribution using External FTP server.

For more information, see Supported Devices for FTP.

If you have selected Using External FTP server option:

Step 1 Enter the following FTP credentials in their applicable text boxes:

Field	Description
FTP Server Name	Name of the FTP server
FTP User Name	FTP Username to access the External FTP server.

Field	Description
FTP Password	FTP Password to access the External FTP server.
Image Location	Location of the image in the FTP server directory. These images will be used by Software Management to upgrade the software images on the selected devices.

Software Management will validate the FTP credentials and image location only while the job is running; not while the job is being scheduled.

If you have selected Using External TFTP server option, proceed to the TFTP Wizard.

Step 2 Click **Next.**

The Remote Staging and Distribution dialog box appears.

Step 3 Select:

a. An image from the Image Selection pane.

b. Click on **Select Applicable Devices** button to automatically select the applicable devices

Or

Manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see Unsupported Software Images.

Step 4 Click **Next**.

If you have selected Using External TFTP server option, proceed to the TFTP Wizard.

The External FTP Server Details dialog box appears with the following details:

Field	Description
IP Address	IP Address of the External FTP server.
Selected Image	Image name that you have selected for distribution.
Errors	Error information.

Step 5 Click **Next**.

If you have selected Using External TFTP server option, proceed to the TFTP Wizard.

The Device Recommendation dialog box appears with the following details:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of recommended image storage information.
Errors	Error information.

Step 6 Click **Next**.

If you have selected Using External TFTP server option, proceed to the TFTP Wizard.

The Remote Devices Verification dialog box appears with the following details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Step 7 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 8 Enter the following information. If you have selected Using External TFTP server option, proceed to the TFTP Wizard.

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (using remote staging) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Field	Description
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If running image is in repository, select option to place a copy in the FTP server directory. Uses this copy if reboot with new image fails. Note the following: • This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in FTP server directory so that device can find it any time it reboots
Back up current running image	Select to back up running image in software image repository before upgrading. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do *not* select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (**Inventory > Device Administration > Add / Import / Manage Devices**) are ignored. You are allowed to provide a password in this field only if you have selected the Enable Job Based Password in the View / Edit Preferences dialog box. See *Administration of Cisco Prime LAN Management Solution 4.1* for more details.

Field	Description
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and the Down arrows to order your devices list. 3. Click **Done**.

Step 9 Click **Next** after you finish entering the job information details. If you have selected Using External TFTP server option, proceed to the TFTP Wizard.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Details of the Remote Stage device or the External FTP server.
- Verification warnings generated during image distribution (if applicable).

Step 10 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Supported Devices for FTP

Table 8-7 Supported Devices for FTP

Device Family	Device	SysObject ID
NAM	NAM X6380	1.3.6.1.4.1.9.5.1.3.1.1.2.223
	NAM1	1.3.6.1.4.1.9.5.1.3.1.1.2.914
	NAM2	1.3.6.1.4.1.9.5.1.3.1.1.2.291
	NM NAM	1.3.6.1.4.1.9.1.562
	NME NAM	1.3.6.1.4.1.9.1.826
WLSE	WLSE	1.3.6.1.4.1.9.1.459
	WLSE	1.3.6.1.4.1.9.1.630
	WLSE	1.3.6.1.4.1.9.1.631
	WLSE 1153	1.3.6.1.4.1.9.1.752
Cisco Catalyst 3750 Series Switches	CatalystIOS37XXStack	1.3.6.1.4.1.9.1.516
	Catalyst3750ME	1.3.6.1.4.1.9.1.574
	WS.C3750G.12S.SD	1.3.6.1.4.1.9.1.688
	WS.C3750E.24TD	1.3.6.1.4.1.9.1.789
	WS.C3750E.48TD	1.3.6.1.4.1.9.1.790
	WS.C3750E.48PD	1.3.6.1.4.1.9.1.791
	WS.C3750E.24PD	1.3.6.1.4.1.9.1.792
	catalyst375024	1.3.6.1.4.1.9.1.511
	catalyst375048	1.3.6.1.4.1.9.1.512
	catalyst375024TS	1.3.6.1.4.1.9.1.513
	catalyst375024T	1.3.6.1.4.1.9.1.514
	catalyst375048PS	1.3.6.1.4.1.9.1.535
	catalyst3750G24PS	1.3.6.1.4.1.9.1.602
	catalyst3750G48PS	1.3.6.1.4.1.9.1.603
	catalyst3750G48TS	1.3.6.1.4.1.9.1.604
	catalyst3750G24TS1U	1.3.6.1.4.1.9.1.624
	catalyst375024FS	1.3.6.1.4.1.9.1.656
Cisco Intelligent Gigabit Ethernet Switch Module (IEGSM)	ciscoIGESM	1.3.6.1.4.1.9.1.592
	ciscoIGESMSFP	1.3.6.1.4.1.9.1.660

Table 8-7 Supported Devices for FTP

Device Family	Device	SysObject ID
Cisco Catalyst 3560,C3560E Series Switches	CatalystIOS3560G.24PS	1.3.6.1.4.1.9.1.614
	CatalystIOS3560G.24TS	1.3.6.1.4.1.9.1.615
	CatalystIOS3560G.48PS	1.3.6.1.4.1.9.1.616
	CatalystIOS3560G.48TS	1.3.6.1.4.1.9.1.617
	CatalystIOS3560.24PS.S	1.3.6.1.4.1.9.1.563
	CatalystIOS3560.48PS	1.3.6.1.4.1.9.1.564
	CatalystIOS3560.24TS	1.3.6.1.4.1.9.1.633
	CatalystIOS3560.48TS	1.3.6.1.4.1.9.1.634
	WS.C3560E.24TD	1.3.6.1.4.1.9.1.793
	WS.C3560E.48TD	1.3.6.1.4.1.9.1.794
	WS.C3560E.24PD	1.3.6.1.4.1.9.1.795
	WS.C3560E.48PD	1.3.6.1.4.1.9.1.796
	WS.C3560.8PC	1.3.6.1.4.1.9.1.797
	WS-C3560E-12D-S	1.3.6.1.4.1.9.1.930
	WS-C3560E-12SD-E	1.3.6.1.4.1.9.1.956
	WS-C3560-12PC-S	1.3.6.1.4.1.9.1.1015
Cisco Blade Switches (CBS)	CBS3030Del	1.3.6.1.4.1.9.1.749
	CBS3020	1.3.6.1.4.1.9.1.748
	CBS3040	1.3.6.1.4.1.9.1.784
	CBS1100	1.3.6.1.4.1.9.1.946
	CBS3110	1.3.6.1.4.1.9.1.947
	CBS3120	1.3.6.1.4.1.9.1.948
	CBS3130	1.3.6.1.4.1.9.1.949
	CBS3012	1.3.6.1.4.1.9.1.999
	CBS3012I	1.3.6.1.4.1.9.1.1000
	CBS3132	1.3.6.1.4.1.9.1.920
	CBS3110G-S	1.3.6.1.4.1.9.1.909
	CBS3110X-S	1.3.6.1.4.1.9.1.910
	CBS3110G-S-I	1.3.6.1.4.1.9.1.911
	CBS3110X-S-I	1.3.6.1.4.1.9.1.912
	CBS3125G-S	1.3.6.1.4.1.9.1.1001
	CBS3120G-S	1.3.6.1.4.1.9.1.918
	CBS3125X-S	1.3.6.1.4.1.9.1.1002
	CBS3120X-S	1.3.6.1.4.1.9.1.919
	CBS3130G-S	1.3.6.1.4.1.9.1.921
	CBS3130X-S	1.3.6.1.4.1.9.1.922

Table 8-7 Supported Devices for FTP

Device Family	Device	SysObject ID
Cisco Catalyst 2960 Series Switches	Catalyst296024	1.3.6.1.4.1.9.1.694
	Catalyst296048	1.3.6.1.4.1.9.1.695
	Catalyst2960G24	1.3.6.1.4.1.9.1.696
	WS-C2960G-48TC-L	1.3.6.1.4.1.9.1.697
	Catalyst296024TT	1.3.6.1.4.1.9.1.716
	Catalyst296048TT	1.3.6.1.4.1.9.1.717
	Catalyst29608TC	1.3.6.1.4.1.9.1.798
	Catalyst2960G8TC	1.3.6.1.4.1.9.1.799
	C2960-24-S	1.3.6.1.4.1.9.1.929
	C2960-24TC-S	1.3.6.1.4.1.9.1.928
	C2960-48TC-S	1.3.6.1.4.1.9.1.927
	C2960-24PC-L	1.3.6.1.4.1.9.1.950
	C2960-24LT-L	1.3.6.1.4.1.9.1.951
	C2960PD-8TT-L	1.3.6.1.4.1.9.1.952
	C2960P	1.3.6.1.4.1.9.1.1006
	C2960	1.3.6.1.4.1.9.1.1005
Cisco Catalyst 3550 Series Switches	Catalyst355012T	1.3.6.1.4.1.9.1.368
	Catalyst355024switch	1.3.6.1.4.1.9.1.366
	Catalyst355048switch	1.3.6.1.4.1.9.1.367
	Catalyst355012G	1.3.6.1.4.1.9.1.431
	Catalyst355024DC	1.3.6.1.4.1.9.1.452
	Catalyst355024FX	1.3.6.1.4.1.9.1.453
	Catalyst355024PWR	1.3.6.1.4.1.9.1.485
Cisco PIX Series Security Appliances	PIX 535	1.3.6.1.4.1.9.1.675
	PIX 525	1.3.6.1.4.1.9.1.676
	PIX 515	1.3.6.1.4.1.9.1.678
	PIX 515E	1.3.6.1.4.1.9.1.451
	PIX 515EFirewall	1.3.6.1.4.1.9.1.677

Table 8-7 Supported Devices for FTP

Device Family	Device	SysObject ID
Cisco Adaptive Security Appliances (ASA)	ASA5510	1.3.6.1.4.1.9.1.773
	ASA5520	1.3.6.1.4.1.9.1.671
	ASA5520	1.3.6.1.4.1.9.1.670
	ASA5510	1.3.6.1.4.1.9.1.669
	ASA5505	1.3.6.1.4.1.9.1.745
	ASA5550	1.3.6.1.4.1.9.1.763
	ASA5540	1.3.6.1.4.1.9.1.673
	ASA5580	1.3.6.1.4.1.9.1.672
	ASA5550	1.3.6.1.4.1.9.1.753
	ASA5540	1.3.6.1.4.1.9.1.914
	ASA5580	1.3.6.1.4.1.9.1.915

Using External TFTP Server

If you have selected Using External TFTP server option:

Step 1 Enter the external TFTP server IP address in the Enter TFTP IP Address text box.

Step 2 Click **Next.**

The Remote Staging and Distribution dialog box appears.

Step 3 Select:

a. An image from the Image Selection pane.

b. Click on **Select Applicable Devices** button to automatically select the applicable devices

Or

Manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see Unsupported Software Images.

Step 4 Click **Next**.

The External TFTP Server Details dialog box appears with the following details:

Field	Description
IP Address	IP Address of the External TFTP server.
Selected Image	Image name that you have selected for distribution.
Errors	Error information.

Step 5 Click **Next**.

The Device Recommendation dialog box appears with the following details:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of recommended image storage information.
Errors	Error information.

Step 6 Click **Next**.

The Remote Devices Verification dialog box appears with the following details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Step 7 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 8 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (using remote staging) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Comments	Enter the additional information about this job.

Field	Description
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following: • This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots
Back up current running image	Select to back up running image in software image repository before upgrading. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do *not* select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.

Field	Description
Enable Job Password	Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (**Inventory > Device Administration > Add / Import / Manage Devices**) are ignored. You are allowed to provide a password in this field only if you have selected the Enable Job Based Password in the View / Edit Preferences dialog box. See *Administration of Cisco Prime LAN Management Solution 4.1* for more details.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and the Down arrows to order your devices list. 3. Click **Done**.

Step 9 Click **Next** after you finish entering the job information details

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Details of the Remote Stage device or the External TFTP/FTPserver.
- Verification warnings generated during image distribution (if applicable).

Step 10 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration** > **Tools** > **Software Image Management** > **Jobs**.

Using Remote Stage Device

If you have selected Remote Stage device option:

Step 1 Go to the Select Remote Stage Device pane, select a device that you want to use as the remote stage device. Ensure that you select a device that supports remote staging.

If you select a device that does not support remote staging, an error message is displayed.

Step 2 Click **Next.**

The Remote Staging and Distribution dialog box appears.

Step 3 Select:

a. An image from the Image Selection pane.

b. Click **Select Applicable Devices** to automatically select the applicable devices

or

Manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see Unsupported Software Images.

Step 4 Click **Next**.

The Remote Stage and Image Upgrade Details dialog box appears with the following details:

Field	Description
Remote Stage Name	Name of the remote stage device that you want to use as a remote stage.
Selected Image	Image name that you have selected for distribution.
Storage Options	Image storage information

Step 5 Click **Next**.

If the Remote Stage verification fails, check if the Remote Stage device has enough free space and restart the software distribution from the beginning.

The Device Recommendation dialog box appears. This displays the following details:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of recommended image storage information.

Step 6 Click **Next**.

The Remote Devices Verification dialog box appears with the following details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Step 7 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 8 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (using remote staging) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Comments	Enter the additional information about this job.

Field	Description
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following: • This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots
Back up current running image	Select to back up running image in software image repository before upgrading. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do *not* select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.

Field	Description
Enable Job Password	Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (**Inventory > Device Administration > Add / Import / Manage Devices**) are ignored. You are allowed to provide a password in this field only if you have selected the Enable Job Based Password in the View / Edit Preferences dialog box. See *Administration of Cisco Prime LAN Management Solution 4.1* for more details.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and the Down arrows to order your devices list. 3. Click **Done**.

Step 9 Click **Next** after you finish entering the job information details

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Details of the Remote Stage device or the External TFTP server.
- Verification warnings generated during image distribution (if applicable).

Step 10 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Unsupported Software Images

During remote staging, there maybe software images running on the devices selected for remote staging, but some of them may not get listed as available images. This is because, some software images do not support Remote Staging and Distribution.

The following below lists the software images that do not support Remote Staging and Distribution:

- CSS_SW FDDI_CDDI
- ATM_WTALL
- ATM_WBPVC
- CIP
- CSS_11000_SW
- C6KMODULE_MWAM_SW
- PATCH_SW
- ONS15530
- TOKENRING
- ATM_WBLANE
- BOOT_LOADER
- C6KMODULE_MWAM_SW
- CSS_11500_SW
- CSS_11000_SW
- C2500
- C1600
- BLADERUNNER
- ATM_WTOKEN
- MICA MICROCOM
- NAM_APPL_SW
- SPA_FPD_SW
- CSS_11500_SW
- ONS15540

Understanding Upgrade Recommendations

This section describes how Software Management recommends image for the various Cisco device types:

- Upgrade Recommendation for Cisco IOS Devices
- Upgrade Recommendation for Catalyst Devices
- Upgrade Recommendation for VPN 3000 Series
- Upgrade Recommendation for Catalyst 1900/2820
- Upgrade Recommendation for Other Device Types

Upgrade Recommendation for Cisco IOS Devices

To determine the recommended software images for Cisco IOS devices, Software Management:

1. Lists all images in the software repository that can run on the device. For example, C7000 images run on 7000 and 7010 devices, IGS images run on 25xx devices, and so on.
2. Removes all listed images that require:
   - More RAM or Flash memory than is available on the device.
   - A newer boot ROM than the one on the device.

   If RAM is UNKNOWN, it is not considered in any comparison operation (image filtering). However, you are warned during the subsequent task.
3. Recommends an image whose feature subset matches the image running on the device.
   - Any images that support all current features and include some additional ones, take precedence over images that match exactly.
   - If more than one image is either a superset or an exact match of the running image, the latest version takes precedence over earlier versions.
4. Removes the images from recommendation if the images Min.Flash size requirement is not met by the device.

   If Min.Flash required is UNKNOWN, it is not considered in any comparison operation (image filtering).

   If Flash Size is UNKNOWN, the image cannot be used for upgrade.

   See the IOS Software Release documentation on Cisco.com to know the Min.Flash size.
5. Depending on the image feature list, Software Management recommends an image whose image version is lower than the current running image version.
6. Recommends to filter out the images that are larger in size than the flash available on the device.
7. Recommends Flash partitions on the device along with the storage details, if you are upgrading the Boot Loader image.

This algorithm might recommend images that are older than the one running on the device.

To ensure that only newer images are recommended, select **Admin > Network > Software Image Management > View/Edit Preferences**. In the View/Edit Preferences dialog box, select the Include images higher than running image checkbox, then click **Apply**.

Upgrade Recommendation for Catalyst Devices

For Catalyst device upgrades, Software Management typically recommends the latest version images in the software repository.

For default RAM requirements for Supervisor Engine I and Supervisor Engine III, however, Software Management uses:

Module Type and Version	Default RAM (MB)
Supervisor Engine III	32
Supervisor version 2.1 up to (but not including) 3.1	8
Supervisor version 3.1.1 and later	16
Maintenance release versions 3.1 and 3.2 with “Sup8M” in filename	8

For supervisor versions 3.1 to 3.2, when the image repository or Cisco.com has both 8 MB of RAM and regular images available, Software Management also checks the device RAM:

1. If the RAM can be determined and the available RAM is greater than 16 MB:

a. Software Management recommends the latest regular supervisor image where the RAM requirement is less than the available RAM.

b. If no regular image with matching RAM requirements is available, it recommends the latest version of the 8-MB images.

c. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).

2. If the RAM can be determined and the available RAM is less than 16 MB:

a. Software Management recommends the highest image version for which the RAM requirement is less than 16 MB.

b. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).

3. If the RAM cannot be determined:

a. Software Management recommends the latest regular image.

b. If no regular image is available, it recommends the latest 8-MB image.

c. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).

The minimum RAM in the image attributes file supersedes these guidelines.

For example, if a supervisor engine module is running the version 3.1 maintenance release (8 MB RAM) but the RAM in the image attributes was changed to 16 MB, Software Management uses the value in the attributes file.

Upgrade Recommendation for VPN 3000 Series

Software Management recommends the latest version of the image in the software image repository. If the device is a VPN 3005 Concentrator, it recommends the VPN 3005 System software images in the repository.

Upgrade Recommendation for Catalyst 1900/2820

For Catalyst 1900/2820 Enterprise version device upgrades, Software Management typically recommends the latest version of images in the software repository.

Note For Catalyst 1900/2820 Series devices, Software Management recommends images with version numbers greater than 8.0(0) because the older versions do not support the Command Line Interface. Non-Enterprise versions of the Catalyst 1900/2820 are not supported in Software Management.

Upgrade Recommendation for Other Device Types

For the following device types, Software Management recommends the latest version of the image in the software image repository:

- PIX Firewall Devices

  If you are running PIX image version 7.0 or later, while recommending the image, Software Management will also recommend the storage details of the device.
- Content Service Switches
- Aironet AP Series
- Optical Switch Series
- Network Analysis Module Series
- Content Engines

Using Software Management Job Browser

Using this window you can view all your scheduled Software Management jobs.

The Software Management Job Browser contains the following fields and buttons:

- Software Management Job Browser Fields
- Software Management Job Browser Buttons

This section contains:

- Changing the Schedule of a Job
- Retry a Failed Distribution Job
- Undo a Successful Distribution Job
- Stopping a Job
- Deleting Jobs

The Software Management Job Browser displays the following details for a job:

Table 8-8 Software Management Job Browser Fields

Field	Description
Job ID	Unique number assigned to the job when it is created. Click to display a summary of job details and schedule options. See Understanding the Software Management Job Summary for further details.
Job Type	Type of job such as Import Images, Distribute Images.
Status	Job states: • Successful—Job completed successfully • Failed—Failed job. Click on the Job ID to view the job details. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed is 5. • Running—Job still running. • Pending—Job scheduled to run. • Stopped—Running job stopped by you. • Missed Start—Job could not run for some reason at the scheduled time. For example, if the system was down when the job was scheduled to start, when the system comes up again, the job does not run. This is because the scheduled time for the job has elapsed. The status for the specified job will be displayed as `Missed Start`. • Approved—Job approved by an approver • Rejected—Job rejected by an approver. Click on the Job ID to view the rejection details. • Waiting for Approval—Job waiting for approval.
Description	Job description as entered at the time of creation.
Owner	User who created the job.
Scheduled At	Start time of the scheduled job.
Completed At	End time of the scheduled job.
Schedule Type	Type of the scheduled job: • Immediate • Once

Table 8-9 Software Management Job Browser Buttons

Buttons	Description
Edit	Reschedules the job. You can change the schedule only for jobs that are in the Pending, Waiting for Approval or the Approved status. See Changing the Schedule of a Job.
Retry	Retry the failed job. You can retry only failed distribution jobs. See Retry a Failed Distribution Job.
Undo	Undo a successful job. You can undo only successful distribution jobs. See Undo a Successful Distribution Job. However, you cannot undo a successful software distribution job scheduled for NAM devices. If you still try to Undo this job, an error message is displayed indicating that the Undo operation is not supported for NAM devices.
Stop	Stops a scheduled job. You can Stop only jobs that are either in the Pending or the Running status. See Stopping a Job.
Delete	Delete the jobs. See Deleting Jobs.
Refresh (Icon)	Click on this icon to refresh the Software Management Job Browser Window.

Changing the Schedule of a Job

You can change the schedule only for jobs that are either in the Pending, Waiting for Approval or the Approved status.

Note View Permission Report (**Reports** > **System** > **Users** > **Permission**) to check if you have the required privileges to perform this task.

To change the schedule of a job:

Step 1 Select **Configuration** > **Tools** > **Software Image Management** > **Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select either a pending or an approved job.

Step 3 Click **Edit**.

The Change Job Schedule dialog box appears.

Step 4 Change the schedule.

Step 5 Click **Submit**.

Retry a Failed Distribution Job

You can retry only failed distribution jobs.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To retry a Job:

Step 1 Select **Configuration > Tools > Software Image Management > Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select a failed distribution job.

Step 3 Click **Retry**.

The Retry Upgrade dialog box appears with the following information:

Field	Description
Device Information	Name of the device
Module	Device module
Pre-upgrade Image	Image name that was running before the upgrade.
Selected Image	Image name that is selected for distribution.
Running Image	Image name that is currently running on the device.
Errors	Click on the underlined Error message to review the details.

Step 4 Click **Next**.

Continue entering the information for this job as you would for a new distribution depending on your previous distribution selection:

- Distributing by Devices [Basic]
- Distributing by Devices [Advanced]
- Distributing by Images
- Remote Staging and Distribution

Undo a Successful Distribution Job

You can undo only successful Distribution jobs.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To undo a job:

Step 1 Select **Configuration > Tools > Software Image Management > Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select a successful distribution job.

Step 3 Click **Undo**.

The Undo Upgrade dialog box appears with the following information:

Field	Description
Device	Name of the device
Module	Device module
Pre-upgrade Image	Image name which was running before the upgrade.
Post-upgrade Image	Image name after completing the upgrade.
Running Image	Image name that is currently running on the image.
Errors	Click on the underlined Error message to review the details.

Step 4 Click **Next**.

Continue entering the information for this job as you would for a new distribution. This depend on what you selected earlier in the Distribution Method window:

- Distributing by Devices [Basic]
- Distributing by Devices [Advanced]
- Distributing by Images
- Remote Staging and Distribution

Stopping a Job

You can stop only jobs that are either in the Pending or the Running status.

The job stops only after the current task is complete. During this time, the Software Management Job Browser window displays the job status as Running.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To stop a job:

Step 1 Select **Configuration > Tools > Software Image Management > Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select either a pending or a running job.

Step 3 Click **Stop**.

A confirmation box shows that the selected job will be stopped.

Step 4 Click **OK**.

A message appears that the selected job has been stopped.

After the job is stopped, the Pending job status changes to Stopped. The Running job status changes temporarily to Stop Initiated and then to Stopped.

Deleting Jobs

To delete jobs:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Configuration > Tools > Software Image Management > Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select the jobs.

Step 3 Click **Delete**.

A confirmation box shows that the selected jobs will be deleted.

Step 4 Click **OK**.

Understanding the Software Management Job Summary

From the Software Management Job Browser, you can learn more about one job by viewing its details. You can view this details by clicking the Job ID on the Software Management Job Browser window.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

The Software Management Job Details window contains the following information:

Page/Folder	Description
Work Order	Select a device to view the summary of the job: • If there is more than one device, the software distribution order. • The state of the running image on the device. • The image selected for the upgrade. • Whether Flash memory will be erased before the new image is loaded. • Operations that will be performed during the upgrade procedure. • For a bootloader upgrade, whether the bootloader will be upgraded. • The Job Approval information. • Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device. • Details of the Remote Stage device (if applicable). • Verification warnings generated during image distribution (if applicable).
Job Results	Select a device to view the complete job result. It displays information on: • The job status, start time and end time. • The job completion status on the devices you have selected. For example, number of successful devices where the job is executed successfully. • The import/upgrade mode (parallel or sequential) • The protocol order used for image transfer and configuration tasks. • How the job was processed.
Summary[On Job Complete]	Displays the summary of the completed job For software distribution jobs, the summary contains details about the device, image type, running image name, upgrade image name, upgrade storage location, and image distribution status. For software import jobs, the summary contains details about device, image name, storage location, and import status of the image. The Job Summary is not generated for Image Out-Of-Sync Report job.

Understanding User-supplied Scripts

User-supplied scripts are run before and after each device upgrade, for example:

- The preupgrade script can check whether the device is accessible.
- The preupgrade script can check whether any users are connected to the access server. If the script finds that some users are connected, it can decide whether to disable the connections before upgrading.
- The post-upgrade script can check whether the upgrade was successful. Depending on the return value, Software Management either halts or continues with the rest of the upgrade.

The following sections contain:

Script Requirements

- In the Edit Preferences dialog box (**Admin > Network > Software Image Management > View/Edit Preferences**), enter:
  - Enter the shell scripts (*.sh) on UNIX and batch files (*.bat) on Windows.

    On UNIX, the scripts should have read, write, and execute permissions for the owner (casuser) and read and execute permissions for group casusers. That is, the script should have 750 permission.

    On Windows, the script should have read, write, and execute permissions for casuser/Administrator.

    The other users should have only read permission. You must ensure that the scripts contained in the file has permissions to execute from within the *casuser* account.
  - The script files *must* be available at this location:

    On Solaris and Soft Appliance:

    /var/adm/CSCOpx/files/scripts/swim

    On Windows:

    NMSROOT\files\scripts\swim
  - User script timeout

    Software Management waits for the time specified before concluding that the script has failed.
- Software Management verifies that:
  - The script has write and execute permissions for the user *casuser*.
  - Only users logged in as Administrator, root, or *casuser* have write and execute permissions.

Caution The script should not write output to the system console. The script can write the output to a file. Writing the script output to the system console can cause the Software Management job to hang.

Script Parameters

Software Management passes a parameter indicating whether the script is running before or after the upgrade. If the script does not intend to perform any pre-upgrade check, the script can return an exit value of zero and perform checks in the post-upgrade. See the Sample Script for reference.

The parameters provided to the script by Software Management are in the form of environment variables.

The server environment variables such as *PATH*, *SystemRoot*, etc., are not passed on to the script by Software Management. You have to set the relevant environment variables within the script. See the Sample Script for reference.

See Adding Devices to the Device and Credential Repository section in the *Inventory Management with Cisco Prime LAN Management Solution 4.1* for further information on device hostname, device name (device display name), SNMP v2 community strings, etc.

The different parameters are described in the table below:

Variable	Description
CRM_SCRIPT_CONTEXT	This variable is used to determine if the script has to be invoked before or after image upgrade. If you set the variable to, • PRE-DOWNLOAD—Script is invoked by Software Management prior to image upgrade. • POST-DOWNLOAD—Script is invoked by Software Management post image upgrade.
NMSROOT	LMS installed directory.
TMPDIR	Directory provided to LMS to create temporary files.
CRM_DEV_NAME	Name of Device Display name as entered in Device and Credential Repository.
CRM_SNMP_V2_RWCOMMUNITY	SNMP version 2 read-write community string.
CRM_SNMP_V2_ROCOMMUNITY	SNMP version 2 read only community string.
CRM_SNMP_V3_ENGINE_ID	SNMP version 3 Engine ID
CRM_SNMP_V3_USER_ID	User ID configured for SNMP version 3 protocol access on the device.
CRM_SNMP_V3_PASSWORD	SNMP version 3 password for the user ID.
CRM_ENABLE_PASSWORD	Enable password.
CRM_PRIMARY_USERNAME	Primary user name configured on the device.
CRM_PRIMARY_PASSWORD	Primary password configured on the device.
CRM_DEV_MGMT_IP_ADDR	IP address provided in Device and Credential Repository for management.

Sample Script

The sample script illustrates how to use this option before the upgrade to see if the device is accessible and after the upgrade to see whether it was successful.

The *sample.bat* file contains:

```
c:\progra~1\cscopx\bin\perl c:\progra~1\cscopx\files\scripts\swim\samplescript.pl
```

The *samplescript.pl* file contains:

```
#!/usr/bin/perl
BEGIN
{
use lib "$ENV{NMSROOT}/objects/perl5/lib/Net";

}
use Net::Telnet;
#my $output="";
## The following Environment variables are not passed on by Software Image Management
## Need to set these variables for the script to work as expected
$ENV{'Path'}="C:\\PROGRA~1\\CSCOpx\\MDC\\tomcat\\bin;C:\\PROGRA~1\\CSCOpx\\MDC\\Apache;C:\\PROGRA~1\\CSCOpx\\
MDC\\jre\\bin;C:\\PROGRA~1\\CSCOpx\\MDC\\bin;C:\\PROGRA~1\\CSCOpx\\lib\\jre\\bin\\server;C:\\PROGRA~1\\CSCOpx
\\objects\\db\\win32;C:\\PROGRA~1\\CSCOpx\\bin;c:\\cscopx\\lib\\jre\\bin\\server;c:\\cscopx\\lib\\jre141\\bin
\\server;C:\\WINNT\\system32;C:\\WINNT;C:\\WINNT\\System32\\Wbem;C:\\Program Files\\Common Files\\Adaptec
Shared\\System;c:\\progra~1\\cscopx;c:\\progra~1\\cscopx\\bin;";
$ENV{'TEMP'}=$ENV{'TMPDIR'};
$ENV{'TMP'}=$ENV{'TMPDIR'};
$ENV{'SystemRoot'}="C:\\WINNT";
######  Required Environment variables are set #########
my $prmptchar = '/\>/i';
$filename = $ENV{'CRM_DEV_NAME'} . '.txt';
if ($ENV{'CRM_SCRIPT_CONTEXT'} eq  'PRE-DOWNLOAD') {
open OUTFILE, "> $filename" or die "Can't open file";
print OUTFILE %ENV;

my $host = $ENV{'CRM_DEV_MGMT_IP_ADDR'};
my $pwd = $ENV{'CRM_PRIMARY_PASSWORD'};
print OUTFILE $host;
print OUTFILE $pwd;
$telnet = new Net::Telnet(Input_Log=>"inp.txt");
$prev = $telnet->host($host);
print OUTFILE $prev;
print OUTFILE "Conntecting to Host....";
$telnet->open($host);
print OUTFILE "Connected ...";
$telnet->dump_log("dmp.txt");
$telnet->waitfor('/Username: $/i');
$telnet->print($ENV{'CRM_PRIMARY_USERNAME'});
$telnet->waitfor('/Password: $/i');
$telnet->print($pwd);
print OUTFILE "Password send";
($output) = $telnet->waitfor('/#$/i');
print OUTFILE "Returned after waitfor";
print OUTFILE $output;
$telnet->print('terminal length 0');
$telnet->waitfor('/#$/i');
$telnet->print('sh ver');
($output) = $telnet->waitfor('/#$/i');
print OUTFILE $output;
### If the device is not running the expected Image, return 1
### so that Software Image Management application does not proceed.
if ($output =~ m/Version 12.2\(27\)/) {
    print OUTFILE "Required Software running on Device, Allow to proceed with Upgrade\n"
```

```
    }
else
    {
    print OUTFILE "Upgrade stopped, Device not running desired Image";
    close OUTFILE;
    exit(1);
    }
close OUTFILE;
## A return vale of zero(0) allows the Software Image Management application to proceed
exit(0);
}
if ($ENV{'CRM_SCRIPT_CONTEXT'} eq  "POST-DOWNLOAD") {
my $hostnew = $ENV{'CRM_DEV_MGMT_IP_ADDR'};
my $pwdnew = $ENV{'CRM_PRIMARY_PASSWORD'};
open OUTFILE, ">>$filename" or die "Can't open file";
print OUTFILE "====== POST DOWNLOAD RESULTS ========";
$telnet = new Net::Telnet(Input_Log=>"inp1.txt");
$telnet->dump_log("dmpo.txt");
$telnet->open($hostnew);
$telnet->waitfor('/Username: $/i');
$telnet->print($ENV{'CRM_PRIMARY_USERNAME'});
$telnet->waitfor('/Password: $/i');
$telnet->print($pwdnew);
($opt) = $telnet->waitfor('/#$/i');
$telnet->print('terminal length 0');
$telnet->waitfor('/#$/i');
$telnet->print('sh ver');
($opt) = $telnet->waitfor('/#$/i');
if ($opt =~ m/Version 12.3\(10a\)/) {
    print OUTFILE "Required Software running on Device, Upgrade Successful\n";
}
print OUTFILE $opt;
close OUTFILE;
exit(0);
}
```

Locating Software Management Files

This table shows the locations of some of the Software Management directories and log files that describe what is happening in the system.

Contents	Operating System	Location
Software Management User Interface/job creation debug log file	Solaris and Soft Appliance	/var/adm/CSCOpx/log/swim_debug.log
	Windows	*NMSROOT*\log\swim_debug.log Where *NMSROOT* is the LMS installed directory.
Software Management job execution debug log files. You can set the debug mode for Software Management application in the Log Level Settings dialog box (Admin > System > Debug Settings > Config and Image Management Debugging Settings)	Solaris and Soft Appliance	/var/adm/CSCOpx/files/rme/jobs/swim/*job-id*/swim_debug.log
	Windows	*NMSROOT*\files\rme\jobs\swim*job-id*\swim_debug.log Where *NMSROOT* is the LMS installed directory.

CHAPTER 9

Virtual Switching System Support

Virtual Switching technology is the process of combining two standalone distribution switches found in the local distribution layer into a single management point.

The Virtual Switching System functions and appears as a single switch to the wiring closet and the core layer. You can also create Virtual Switching Systems with a pair of standalone switches available in the core layer.

After the conversion of two distribution switches into one Virtual Switching System, the wiring closet switch creates a port bundle to the Virtual Switching System.

Creating a port bundle allows you to manage Standalone switches, easily because the port bundle has to manage only a single virtual port to the Virtual Switching System.

This Virtual Switching technology is implemented in LAN Management Solutions (LMS) by providing a Virtual Switching System Configuration Tool.

This GUI based conversion tool allows you to select two compatible standalone switches and guides you in converting those standalone switches into one Virtual Switching System.

During the conversion process, the Virtual Switching System Configuration tool generates the required CLI commands, based on your inputs. The process then pushes this configuration to the devices using the protocol order provided in **Admin > Collection Settings > Config > Config Transport Settings**.

This section contains:

Note Only VSS-capable standalone Cisco Catalyst 6000 switches can be converted into a Virtual Switching System.

Prerequisites for Conversion

Before you convert Standalone switches to a Virtual Switching System, you must ensure that:

- Candidate devices that are to be converted to a Virtual Switching System are managed by LMS so that they can use this conversion tool.
- Fresh Inventory and Config Collection has been carried out.
- Only VSS-capable IOS Software Modularity images are running on the Standalone switches.

Virtual Switching System Configuration Process

Two Standalone distribution switches can be converted into a single Virtual Switching System by using the Virtual Switching System Configuration Tool available in LMS. This process of converting to Virtual Switching Systems can also be done for core layer switches.

Before proceeding with conversion, ensure that the prerequisites are met.

For more information, see Prerequisites for Conversion.

To convert standalone switches to a Virtual Switching System:

1. Select Devices for VSS Configuration
2. Perform Hardware Checks on the Devices
3. Perform Software Compatibility Checks on the Two Devices
4. Generate Compliance Report
5. Define Configuration Parameters
6. Deploy Commands on the Two Switches to Enable VSS Mode

Select Devices for VSS Configuration

You need to select two switches and convert them into one Virtual Switching System. Only VSS-capable Standalone devices can be converted to Virtual Switching System.

The Virtual Switching System Configuration Tool consists of a customized device selector. This device selector displays only VSS-capable devices with their sysObjectIDs.

Perform Hardware Checks on the Devices

After you select two devices, sequential hardware checks are carried out by the Virtual Switching System Configuration tool on these two devices to ensure hardware compliance.

The hardware checks carried out are:

- RAM size check

  The RAM sizes in MB of both the devices are compared.

  If you try to convert one device with 450 MB RAM and another device with 512 MB RAM into a Virtual Switching System, a warning message is displayed. However, you are allowed to proceed with the conversion.

- Supervisor Type check

  The Supervisor types of both the devices are compared. You cannot convert one device with Supervisor4 and another device with Supervisor3 into a Virtual Switching System. Only Supervisor4 is supported for VSS Configuration.

- Modules not supported in VSS mode

  Ideally, all modules available in the two devices must support VSS mode. Modules in the two devices that do not supprt VSS mode are displayed here.

- Physical Connectivity check

  Both devices should have physical connectivity. This connectivity enables you to convert them to the Virtual Switching System mode.

Perform Software Compatibility Checks on the Two Devices

After the hardware compatibility check is done, the selected devices undergo a software compatibility check.

The software compatibility checks are:

- Switch mode check

  Check whether both devices are in standalone non-VSS modes.

  You cannot convert a Standalone switch and a Virtual-mode configured switch into a Virtual Switching System.

- IOS Software Modularity Image check

  Both devices must be running VSS-capable IOS Software Modularity images in native IOS mode. An image is considered VSS-capable if it has SXH as the last three characters of the image name.

  Example

  The image, 12.2(99)SXH is considered VSS-capable because it has SXH as the last three charaters of the image name.

Generate Compliance Report

After the hardware and software compatibility checks have been completed, a Compliance report is generated. This report indicates the various attributes considered for the checks and the status of the checks.

If there are any instances of non-compliance, you need to restart the conversion process to address these non-compliances.

You are allowed to proceed to the next step only if both hardware and software compatibility checks are successful.

For example:

If the devices do not comply with the minimum IOS software image version, you need to upgrade the software images in the two devices to the minimum recommended version.

A link is provided to the software image upgrade page along with the compliance report, if the minimum software requirement is not met. You can use this link to upgrade the software images in the devices to the minimum IOS software image version.

Define Configuration Parameters

When the devices are made compliant with the hardware and software compability checks, you need to define configuration parameters for both the devices.

The configuration definition includes:

- Specifying the Domain number for the Virtual Switching System configuration
- Assigning one switch as the Active switch and the other as the Standby switch
- Entering the Switch Priority value for both switches

- Entering the Port Channel numbers for both switches
- Selecting 10 Gigabit Ethernet Interfaces for both switches.

Deploy Commands on the Two Switches to Enable VSS Mode

After you have defined the configuration parameters, the Conversion Work Order page is displayed. This page lists the various CLI commands that you must download to the two devices. The CLI commands convert the switches into a Virtual Switching System.

These CLI commands are generated by the Virtual Switching System Configuration tool. You need to deploy the CLI commands on the devices.

LMS uses various protocols such as Telnet, SSH, RCP, SCP, and TFTP to deploy the commands on the devices. The protocols are tried out in the order specified in LMS. If the first protocol in sequence cannot log into the device, the next protocol in the order is tried out, until a suitable protocol is found.

For more information on how to change the protocol order, see *Administration of Cisco Prime LAN Management Solution 4.1*.

The devices reboot after the CLI commands have been deployed on them. One switch is transformed to function as an Active switch and the other as a Standby switch.

After successful conversion, the running configuration of the VSS setup is copied to its startup configuration. The individual switches are then moved to the Suspended state in LMS.

The new Virtual Switching System is added to Device Credentials Repository (DCR) with the display name, same as the IP Address of the Active switch followed by _VSS.

Note After conversion, irrespective of whether an Active or Standby switch boots up first, the conversion to Virtual Switching System takes place successfully. The IP address of the Active device is added to DCR.

Converting Switches from Standalone to VSS Mode

LAN Management Solution (LMS) provides support for Virtual Switching Systems.

You can use the Virtual Switching System Configuration Tool to convert VSS-capable Standalone switches to a Virtual Switching System. This GUI-based tool is a wizard that guides you through the conversion process.

Before you start converting Standalone switches to a Virtual Switching System, you need to ensure that the prerequisites are met.

For more information, see Prerequisites for Conversion.

To convert Standalone switches to a Virtual Switching System:

Step 1 Select **Configuration > Workflows > Virtual Switching System > VSS Conversion**.

The Virtual Switching System Mode Conversion dialog box appears.

Step 2 Select two Standalone switches that are VSS-compliant from the Device Selector to convert to a Virtual Switching System.

The device selector is customized to display only Standalone switches that are VSS-compliant.

Step 3 Click **Convert to VSS Mode**.

- If the switches are compatible, the Checking the Hardware and Software Requirements dialog box appears.
- If the switches are not compatible, an error message is displayed and the conversion is terminated. In this case, you must restart the conversion after making the switches hardware and software compatible.

For more information on the hardware and software checks, see Table 9-1.

Table 9-1 Hardware and Software Check

Properties	Device 1	Device 2
Hardware Checks		
RAM Size	The RAM size in MB for Device 1.	The RAM size in MB for Device 2.
Supervisor Type	The Supervisor type for Device 1.	The Supervisor type for Device 2.
Modules not supported in VSS mode	Names of modules in Device 1 that do not support VSS mode.	Names of modules in Device 2 that do not support VSS mode.
Physical Connectivity	The IP Address through which Device 1 is connected.	The IP Address through which Device 2 is connected.
Result	Status of hardware check.	
Software Checks		
Properties	**Device 1**	**Device 2**
VSS Mode	The current mode of Device 1.	The current mode of Device 2.
Image Version	The software image version in Device 1	The software image version in Device 2.
Result	Status of software check.	

When the RAM size of both the devices are not equal, a warning message is displayed. However, you will be allowed to continue with the conversion.

Step 4 Click **Next**.

The Define Configuration Parameters dialog box appears.

Step 5 Enter the required information as shown in Table 9-2

Table 9-2 Define Configuration Parameters

Field	Description
Virtual Switching System Configuration	
Enter Domain Number	Domain number to be used by the Virtual Switching System, which can be any number between 1 to 255. This domain number is common for both the switches.
Device Name: 1	
Select Switch Number	Either • Check Switch No.1 if you want to assign Device 1 as Switch No. 1. Or • Check Switch No.2 if you want to assign Device 1 as Switch No. 2. You cannot assign both Device1 and Device 2 as Switch No.1. If Device 1 is assigned Switch No.1 then Device 2 should be assigned as Switch No.2. The configuration of the switch designated as No. 2 is overwritten by the configuration of the switch designated as No. 1. The first switch becomes the Active Switch and the second switch becomes the Standby Switch.
Enter Switch Priority	Switch Priority number to be used by the Virtual Switching System, which can be any number between 1 and 255. The switch with the higher value becomes the Active Switch and the other switch becomes the Standby Switch. The priority value should not be the same for both switches.
Enter Port Channel Number	Port Channel for Device 1. Enter a number between 1 and 255. The Port channel number must be different for each switch.

Table 9-2 Define Configuration Parameters

Field	Description
Select Interface	Interface for Device 1. Select the interface for the device from the list box that displays the 10 Gigabit Ethernet interfaces. A minimum of one interface must be selected for the device. Use the Control Key to select more than one interface. Only VSS-capable 10 Gigabit line cards are displayed. Interface modules for Supervisor 4, 6708 10 Gigabit and 6716 10 Gigabit interfaces are available for selection. For 6716 10 Gigabit type cards, only four interfaces are displayed for selection. For example, if there is a 6716 10 Gigabit card in the device, only the following four interfaces (1, 5, 9, 13) are displayed: • TenGigabitEthernet <module number>/1 • TenGigabitEthernet <module number>/5 • TenGigabitEthernet <module number>/9 • TenGigabitEthernet <module number>/13 Where <module number> is the module number of the Gigabit card. For example, TenGigabitEthernet 6/1, where 6 is the module and 1 is the interface. The number of interfaces selected must be the same for both devices.
Device Name: 2	
Select Switch Number	Either: • Check Switch No.1 if you want to assign Device 2 as Switch No. 1. Or • Check Switch No.2 if you want to assign Device 2 as Switch No. 2. You cannot assign both Device1 and Device 2 as Switch No.1. If Device 1 is assigned Switch No.1 then Device 2 should be assigned as Switch No.2. The configuration of the switch designated as No. 2 is overwritten by the configuration of the switch designated as No. 1. The first switch becomes the Active Switch and the second switch becomes the Standby Switch.
Enter Switch Priority	Switch Priority number to be used by the Virtual Switching System, which can be any number between 1 and 255. The switch with higher value becomes the Active Switch and the second switch becomes the Standby Switch. The priority value should not be the same for both switches.

Table 9-2 Define Configuration Parameters

Field	Description
Enter Port Channel Number	The Port channel for Device 2. Enter a port channel number for the switch between 1 and 255. The Port channel number must be different for each switch.
Select Interface	The Interface for Device 2. This list box lists the 10 Gigabit Ethernet interfaces. Select the interface for the device from the list box. At least one interface must be selected for the device. Use the Control Key to select more than one interface. Only VSS capable 10 Gigabit line cards are displayed. Interface modules for Supervisor 4, 6708 10 Gigabit and 6716 10 Gigabit cards are available for selection. For 6716 10 Gigabit type cards, only four interfaces are displayed for selection. For example, if there is a 6716 10 Gigabit card in the device, only the following four interfaces (1, 5, 9, 13) are displayed: • TenGigabitEthernet <module number>/1 • TenGigabitEthernet <module number>/5 • TenGigabitEthernet <module number>/9 • TenGigabitEthernet <module number>/13 Where <module number> is the module number of the Gigabit card. For example, TenGigabitEthernet 6/1, where 6 is the module and 1 is the interface. The number of interfaces selected must be the same for both devices.

Step 6 Click **Next**.

The Work Order page appears with the CLI commands that need to be downloaded to each of the switches so that they can be converted into one Virtual Switching System.

Step 7 Click **Finish**.

- If the conversion was completed, a message is displayed that the two switches have been converted to a single Virtual Switching System.
- If the conversion failed, an error message is displayed indicating the reason for failure. The reason could be that the CLI commands were not properly deployed on the devices.

Note You cannot set priorities for the two Standalone switches that are considered for VSS conversion. Both the Standalone switches have equal priority by default.

Support for Virtual Switching Systems

The various applications in LMS such as Syslog, Inventory Management, Reporting, Software Management, and Configuration Management provide support for Virtual Switching Systems.

The implication of Virtual Switching System support for these applications is discussed below:

- Inventory Management
- Configuration Management
- Syslog
- Software Management - Software Distribution
- Software Management - Scheduling a Software Distribution Job

Inventory Management

The Virtual Switching System is considered as a single switch by Inventory. However Inventory collection happens for both switches.

You can generate a Detailed Device Report for the Virtual Switching System. The output of this report consists of information on both the Active and the Standby switches.

For more information on how to generate a Detailed Device Report, see *Reports Management with Cisco Prime LAN Management Solution 4.1*.

Configuration Management

After the conversion, the Virtual Switching System will have a single unified configuration. Configuration management provides support for Virtual Switching Systems by managing the configuration of the switch.

You can use Configuration Management to:

- Archive the device configurations
- Determine out-of-sync configuration files
- View the configuration version tree
- Compare the revisions of configurations
- Compare the archived configuration with a baseline template
- Deploy a version of configuration on the device

For more information on Configuration Management, see Archiving Configurations and Managing them using Configuration Archive.

You can also use NetConfig and Config Editor to configure Interfaces on a VSS device.

For more information on using NetConfig and Config Editor, see:

- Making and Deploying Configuration Changes Using NetConfig
- Editing and Deploying Configurations Using Config Editor

Syslog

The Syslog messages are sent from the Active switch of the Virtual Switching System to the LMS server. These messages are treated like any other Syslog message from any other device type. Syslog reports can be generated for the Syslogs received from the Active switch of the Virtual Switching System.

For information on Syslogs, see *Administration of Cisco Prime LAN Management Solution 4.1*.

Software Management - Software Distribution

Software Management is enhanced to support distribution of software images to a Virtual Switching System. Software Management uses Master Chassis - Active Supervisor for software distribution.

Software Distribution through LMS Software Management varies based on the software image or Patch image considered for distribution.

- Distribution of the Base Image

  Distributing the software Base image consists of:

  a. Copying the new software image to the Master switch, Flash storage partition.
  b. Copying the same software image to the corresponding slave switch Flash storage partition.

     If Master Flash storage is `disk0` the software image will be copied to `slave-disk0` Flash storage of the Slave switch.
  c. Loading the Active switch.
  d. Loading the Slave switch.
  e. Activating the software image on both the Flash storages.
  f. Rebooting the Master switch.

- Distribution of Patch image

  Distribution of software base image consists of:

  a. Copying of the new patch image to the Master switch, Flash storage partition.
  b. Copying the same Patch image to the corresponding Slave switch, Flash storage partition.

     If Master Flash storage is `disk0,` the Patch image will be copied to `slavedisk0` Flash storage of the Slave switch.
  c. Loading the Active switch.
  d. Loading the Slave switch.
  e. Activating the Patch image on both the Flash storages.

     You are allowed to reload the device to activate the Patch images, only if you have selected Reload if required option while scheduling the Patch distribution job.

  – When you reload, the standby Route Processor(RP) on the Slave switch is reset.
  – The device reboots as soon as the installed code starts running.
  – A manual switchover to the redundant supervisor engine for a dual processor redundant system takes place.

Note You can only distribute Patch images to a Virtual Switching System running VSS-capable IOS Software Modularity image in Install mode.

For more information on Software Distribution, see Software Distribution.

Software Management - Scheduling a Software Distribution Job

Scheduling a Software Management distribution job for Virtual Switching Systems is almost similar to that of any Standalone switch. In addition to the verifications performed by Software management, there are a few verifications that are carried out for Virtual Switching Systems.

Software management verifies:

- If VSS-capable IOS Software Modularity images are running on the devices.

  The prerequisite for VSS is that the devices should have VSS-capable IOS Software Modularity images running on them. So if you select an image that is not a VSS-capable IOS Software Modularity image, the software distribution job cannot be performed.

- If the RAM space available on the two devices are compatible.

  RAM checks are carried out only for Master switch supervisors and not for Slave switch supervisors.

- If there is an identical Slave switch storage partition with enough space for the selected Master switch storage partition.

For more information on Software Distribution, see:

- Distributing by Devices [Basic]
- Distributing by Devices [Advanced]
- Distributing by Images
- Remote Staging and Distribution
- Patch Distribution

Converting Switches from Virtual to Standalone Mode

Virtual Switching System refers to the conceptual switch that is created by converting two VSS-capable standalone switches into one switch. You can also convert Virtual Switching Systems back to Standalone switches.

To convert Virtual Switching Systems into Standalone switches:

Step 1 Locate the original configurations of the two switches.

These configurations maybe available as files on your server. If not, locate them from the Configuration Archive of LMS.

For more information on locating the configurations, see Using the Configuration Version Tree.

You can continue with this procedure even if the original configuration files are not available. You can manually reconfigure the individual switches, if required.

Step 2 Back up the current VSS setup configuration.

This configuration may be required for future conversions.

Step 3 Connect to the VSS setup using Telnet and:

a. Remove all the loop back interfaces on the VSS.

Run the command `no loopback` for each loop back address on the switch.

This removes the loop back addresses from the switch.

b. Go to the running configuration of the VSS setup and configure the IP address on the physical interface of the Standby switch.

This IP address must be in a subnet that is not the physical interface of the Active switch.

After the IP address is configured on the physical interface, the Standby chassis is accessible through the management IP address.

c. Save this configuration change by running the `write mem` command.

The configuration is saved to the NVRAM of the corresponding device.

d. Run the command `switch convert mode stand-alone` in Enable mode.

This command will reload the Active switch and release the switch from VSS setup.

Step 4 Connect to the VSS setup using Telnet. You must use the IP address configured in Step 3b.

Step 5 Run the command `switch convert mode stand-alone` in Enable mode.

The switches are now in Standalone mode. You can access them using their own management addresses.

Step 6 Either:

- Add the two devices to the DCR of LMS, if they do not exist there. To do this select **Inventory > Device Administration > Add / Import / Manage Devices.**

Or

- Change the device states if the devices are in Suspended state. This change allows the two devices to be managed again by LMS.

Note Alternatively, you can refer to the VSS Reverse Conversion wizard for the procedures for converting Virtual Switching Systems to Standalone switches. To access the wizard, go to **Configuration > Workflows > Virtual Switching System > VSS Reverse Conversion**.

Use Case: Converting Standalone Switches into a Virtual Switching System

Case:

You are a network administrator and you want to convert two standalone switches into a Virtual Switching System by using the Virtual Switching System Configuration Tool available in LMS.

Solution:

To convert Standalone switches to a Virtual Switching System:

Step 1 Select **Configuration > Workflows > Virtual Switching System > VSS Conversion**.

The Virtual Switching System Configuration dialog box appears.

Step 2 Select 10.77.118.242 and 10.77.118.242_alias, two Standalone switches that are VSS-compliant, from the Device Selector to convert to a Virtual Switching System.

Step 3 Click **Convert to VSS Mode**.

You can view the hardware and software check results.

Step 4 Click **Next**.

The Define Configuration Parameters dialog box appears.

Step 5 Enter the required information in the Define Configuration Parameters dialog box.

Step 6 Click **Next**.

The Work Order page appears with the CLI commands that need to be downloaded to each of the switches so that they can be converted into one Virtual Switching System.

Step 7 Click **Finish**.

A message is displayed that the two switches have been converted to a single Virtual Switching System.

After successful conversion, the running configuration of the VSS setup is copied to its startup configuration. The individual switches are then moved to the Suspended state in LMS.

The new VSS switch is added to the Device Credentials Repository (DCR) with the display name, same as the IP address of the Active switch followed by _VS

So, the IP address of the Virtual Switching System is **10.77.118.242_VSS**

CHAPTER 10

Configuring VLAN

LMS collects data about devices so that you can configure and manage Virtual Local Area Network (VLAN) in your network. You must set up your LMS server properly to ensure that Data Collection is successfully performed in your network.

The configuration module in LMS helps you to manage your VLANs. You can configure and manage VLAN, Private VLAN (PVLAN), Trunk, and also assign ports to VLANs.

This section contains:

Understanding Virtual LAN (VLAN)

A VLAN allows you to create logical broadcast domains that can span across a single switch or multiple switches, regardless of physical positioning. A VLAN contains a group of devices on one or more LANs.

These devices are configured in such a way that they can communicate as if they were all on the same network segment. VLANs are based on logical connections instead of physical connections, and hence they are extremely flexible.

VLAN allows you to group ports on a switch to limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN is only flooded out to other ports belonging to that VLAN.

This helps to reduce the size of broadcast domains and it allows groups or users to be logically grouped without being physically located in the same place.

The following topics are covered in this section:

Advantages of VLANs

VLANs provide the following advantages:

Simplification of Adds, Moves, and Changes

Adds, moves, and changes are some of the greatest expenses in managing a network. Many moves require re-cabling and almost all moves require new station addressing and hub and router re-configuration.

VLANs simplify adds, moves, and changes. VLAN users can share the same network address space regardless of their location.

If a group of VLAN users move but remain in the same VLAN connected to a switch port, their network addresses do not change.

If a user moves from one location to another but stays in the same VLAN, the router configuration does not need to be modified.

Controlled Broadcast Activity

Broadcast traffic occurs in every network. Broadcasts can seriously degrade network performance or even bring down an entire network, if the network is not properly managed.

Broadcast traffic in a particular VLAN is not transmitted outside that VLAN. This substantially reduces overall broadcast traffic, frees bandwidth for real user traffic, and lowers the vulnerability of the network to broadcast storms.

You can control the size of broadcast domains by regulating the size of their associated VLANs and by restricting both the number of switch ports in a VLAN and the number of people using the ports.

You can also assign VLANs based on the application type and the amount of application broadcasts. You can place users sharing a broadcast-intensive application in the same VLAN group and distribute the application across the network.

Workgroup and Network Security

You can use VLANs to provide security Firewalls, restrict individual user access, flag any unwanted network intrusion, and control the size and composition of the broadcast domain.

You can:

- Increase security by segmenting the network into distinct broadcast groups.
- Restrict the number of users in a VLAN.
- Configure all unused ports to a default low-service VLAN.

VLAN Components

The VLAN components are:

- Switches that logically segment the end stations connected to it.

  Switches are the entry point for end-station devices into the switched domain and provide the intelligence to group users, ports, or logical addresses into common communities of interest. LAN switches also increase performance and dedicated bandwidth across the network.

  You can group ports and users into communities using a single switch or connected switches. By grouping ports and users across multiple switches, VLANs can span single-building infrastructures, interconnected buildings, or campus networks.

  Each switch can make filtering and forwarding decisions by packet and communicate this information to other switches and routers within the network.

- Routers that extend VLAN communication between workgroups.

  Routers provide policy-based control, broadcast management, and route processing and distribution. They also provide the communication between VLANs and VLAN access to shared resources such as servers and hosts.

  Routers connect to other parts of the network that are either logically segmented into subnets or require access to remote sites across wide area links.

- Transport protocols that carry VLAN traffic across shared LAN.

  The VLAN transport enables information exchange between interconnected switches and routers on the corporate backbone. This backbone acts as the aggregation point for large volume of traffic.

  It also carries end-user VLAN information and identification between switches, routers, and directly attached servers. Within the backbone, high-capacity links with high-bandwidth carry the traffic throughout the enterprise.

Using VLANs

You can use Configuration Management functionality in LMS to create, modify, and delete VLANs. You can use the Topology Services to create Ethernet VLANs.

LMS allows you to modify most of the VLAN characteristics that were entered when you created the VLAN, such as purpose, description, and LANE services.

The following sections brief on the types of VLANs supported by Topology Services:

- Ethernet VLAN (See Ethernet VLANs)
- Private VLANs (See Understanding Private VLAN)

Configuring VLANs

You can configure VLANs using VLAN Configuration wizard.

Creating VLAN

To create VLANs, the VLAN Configuration wizard directs you through:

1. Selecting Devices or Entities
2. Creating VLANs
3. Assigning Ports to VLANs
4. Disallowing VLAN on Trunks
5. Understanding VLAN Creation Summary

Deleting VLAN

To delete VLANs, the VLAN Configuration wizard directs you through:

1. Deleting VLANs
2. Moving Affected Ports to New VLAN
3. Understanding VLAN Deletion Summary

Selecting Devices or Entities

You must select the devices or entities to be included in the VLAN. Domain Selector helps you to select devices in Switch Clouds and VTP Domains.

To select devices or entities for a VLAN:

Step 1 Select **Configuration** > **Workflows** > **VLAN** > **Configure VLAN**.

The VLAN Configuration page appears.

Step 2 Select the devices using the Device Selector or the Domain Selector from the VLAN Configuration dialog box.See Table 10-1

Table 10-1 VLAN Configuration Field Description

Field	Description
Device Selector	Lists all the devices in your network. Click the radio button to select the Device Selector.
Domain Selector	Lists the Switch Clouds and VTP Domains in your network. Click the radio button to select the Domain Selector.
All	Click **All** to view all the devices in the network. Check the checkboxes to select the devices.
Selection	Displays the devices that you have selected in the **All** pane.

Step 3 Either:

a. Click **Create** to create VLANs.

The Create VLAN page appears.

b. Go to Creating VLANs.

Or

a. Click **Delete** to delete the VLANs.

The Select VLAN to Delete page appears.

b. Go to Deleting VLANs.

Creating VLANs

After you select devices using the Device Selector or the Domain Selector and click **Create** in the VLAN Configuration page, the Create VLAN page appears. For more details, see Selecting Devices or Entities.

You must enter the details as described in the Table 10-2.

Table 10-2 Create VLAN Field Description

Field	Description
VLAN Name	Enter a name for the new VLAN.
VLAN Index	Enter a number to identify the VLAN. You can enter a number within the range: • 2 to 1001 • 1025 to 4094 You cannot enter 1 or a number in the range 1002 to 1024, as the VLAN Index. These are reserved numbers.
Create on all transparent switches	Check the checkbox to include all switches that are VTP transparent. VTP transparent switches do not send VTP updates and do not act on VTP updates received from other switches. This checkbox is available only for VTP domain based VLAN creation. For more details on this, see Creating VLANs on Transparent Devices.
Copy running to start-up config	Check the checkbox to copy the running configuration to the start-up configuration.

Click any of the following:

- **Next** to continue.

  The Assign Ports to VLAN page appears. For details, see Assigning Ports to VLANs.

  Assigning ports to VLANs cannot be done for more than 100 devices at a time, since it results in memory issues. If you have selected more than 100 devices, click Finish to save VLAN creation. Do VLAN port assignment for 100 devices at a time.
- **Cancel** to exit.
- **Finish** to save changes.

  VLANs are created on the specified devices and the initial VLAN Configuration page appears.

Creating VLANs on Transparent Devices

When you create VLANS *without* checking the *Create On All Transparent Switches* option in the VLAN creation page, the following is the behavior:

Device Selected	Access and Trunk ports listed in the VLAN Creation flow	VLAN created on
VTPv2 Server	• VTPv2 Server • VTPv2 Client	VTPv2Server
VTPv3 Primary Server	• VTPv3 Server • VTPv3 Client • VTPv3 Primary Server	VTPv3 Primary Server
VTPv2 or VTPv3 Transparent device	Selected Transparent device	Selected Transparent device
Device that has VTPv3 in Off Mode	Selected Off Mode device	Selected Off Mode device

When you create VLANS *with* the *Create On All Transparent Switches* option in the VLAN creation page, the following is the behavior:

Device Selected	Access and Trunk ports listed in the VLAN Creation flow	VLAN created on
VTPv2 Server	• VTPv2 Server • VTPv2 Client • VTPv2 Transparent device	• VTPv2Server • VTPv2 Transparent
VTPv3 Primary Server	• VTPv3 Server • VTPv3 Client • VTPv3 Primary Server • VTPv3 Transparent device • VTPv3 Off Mode device	• VTPv3 Primary Server • VTPv3 Transparent device • VTPv3 Off Mode device
VTPv2 or VTPv3 Transparent device	• VTPv2 or VTPv3 Transparent device • VTPv3 Off Mode device	• VTPv2 or VTPv3 Transparent device • VTPv3 Off Mode device
Device that has VTPv3 in Off Mode	• VTPv3 Transparent device • VTPv3 Off Mode device	• VTPv3 Transparent device • VTPv3 Off Mode device

In the above tables, VTPv2 refers to VTP version 2 and VTP v3 refers to VTP version 3.

Assigning Ports to VLANs

A VLAN created in a management domain remains unused until you assign one or more switch ports to the VLAN.

The Assign VLANs to Port page appears after you create the VLAN name and index.

To assign ports to VLANs:

Step 1 Select **Configuration** > **Workflows** > **VLAN** > **Configure VLAN**.

The VLAN Configuration page appears.

Step 2 Select device or domain from the VLAN Configuration page.

Step 3 Click **Create**.

Step 4 Enter VLAN Name and VLAN Index in the Create VLAN page and click **Next**.

The Assign Ports to VLAN page appears.

Step 5 Select the ports and click **Next**.

Table 10-3 describes the entries in the Assign Ports to VLAN page.

Table 10-3 Assign Ports to VLAN Page Field Description

Field	Description
VLAN	Displays the name of the new VLAN.
Filter	Select any of the following criteria based on which you want to filter the list: • Link • Port • Device Name • Device Address • Port Status • VLAN Index • VLAN Name • Association type Or enter * or leave the field blank and click **Filter** to get all the records.
Advanced Filter	Click **Advanced Filter** to open Advanced Filter dialog box. Advanced filtering allows you to search ports using more search criteria. For more details on Advanced Filter, see Advanced Filter.
Column	
Link	Shows whether the port is connected to a switch or not. The value can either be True or False.
Port	Name of the port.
Device Name	Name of the device to which the port belongs to.
Device Address	IP address of the device to which the port belongs to.
Port Status	Status of the port. Shows whether the port is active or down.

Table 10-3 Assign Ports to VLAN Page Field Description (continued)

Field	Description
VLAN Index	Index number for the VLAN to which the port belongs to.
VLAN Name	Name of the VLAN to which the port belongs to.
Association Type	Type of VLAN association.

Step 6 Click any of the following:

- **Next** to continue.

  The Disallow VLAN on Trunks page appears.
- **Back** to modify the Create VLAN page.
- **Cancel** to exit.
- **Finish** to save changes.

  VLANs are created on the specified devices, selected ports are assigned to new VLAN and the initial VLAN Configuration page appears.

For more details, see Disallowing VLAN on Trunks.

Advanced Filter

The Advanced Filter allows you to filter and choose the ports using various parameters and criteria, for assigning the ports to the VLAN. Table 10-4 describes the fields in the Filter Ports Window, when you click Advanced Filter from the Assign Ports to VLAN Window.

Table 10-4 Filter Ports Field Description

Field	Description
Match All	Select the radio button to filter the ports that match all the selected parameters.
Match Any	Select the radio button to filter the ports that match any of the selected parameter.

Table 10-4 Filter Ports Field Description (continued)

Field	Description
Parameter	Select a parameter for which you want to filter the ports. Parameter is the attribute of a port. The values displayed for Assigning ports to VLANs are: • Device Name • **Device Address** • **Link** • **Port** • **Port Status** • Port Description • **VLAN Index** • **VLAN Name** • **Association Type** The values displayed for Configuring Promiscuous ports are: • **Link** • **Port** • Device Name • **Device Address** • **VLAN Name** • Port Mode
Criteria	Select the right criterion with respect to the parameter. The values are: • **contains** • **begins with** • **ends with** • **is**
Value	Enter a value corresponding to the parameter that you have selected.

Click any of the following:

- **More** to add filter.
- **Fewer** to remove filter from the existing filters.

  You can add or remove only one filter at a time.
- **Filter** to filter the ports based on the values for the Parameters.

Disallowing VLAN on Trunks

You can select the links on which you do not want to allow Trunking in the newly created VLAN. After you Assign the ports to the VLAN (See Assigning Ports to VLANs), the End-to end VLAN wizard directs you to Disallow VLAN on Trunks page.

To disallow trunking on the links in your VLAN, check the checkboxes corresponding to those links, and click **Next**. The VLAN Creation Summary page appears.

Clicking **Back** takes you to the Assign Ports to VLAN page, where you can modify the port assignment.

Clicking **Finish** saves the changes and takes you to the initial VLAN Configuration page**.**

For more details, see Understanding VLAN Creation Summary.

Table 10-5 describes the fields in the Disallow VLAN on Trunks page.

Table 10-5 Disallowing VLAN on Trunks Page Field Description

Field	Description
VLAN	Name of the VLAN.
Port1	Port on the first device linked to the VLAN.
Device1	Name of the first device in the link.
Device1 Address	IP Address of the first device in the link.
Domain1	Domain to which the device belongs to.
Port2	Port on the second device linked to the VLAN.
Device2	Name of the second device in the link.
Device2 Address	IP Address of the second device in the link.
Domain 2	Domain to which the device belongs to.

Understanding VLAN Creation Summary

The VLAN Creation Summary page summarizes the operations that you performed through the VLAN Configuration wizard. The Summary provides the following information:

- VTP Domain—Lists the VTP domains.
- Summary—Lists different parameters that you have entered.
  - VLAN Creation Parameters—Lists the VLAN name and index, and the value of the parameters Create on all transparent switches and Copy running-config to startup-config.
  - VLAN Port Assignment Parameters—Lists the VLAN name and index, and ports to which the VLAN is assigned.
  - VLAN Trunk Configuration Parameters—Lists the Trunks on which the VLAN is allowed or disallowed.

Example:

```
VLAN Creation Parameters

VLAN Name: Test
VLAN Index: 912
Create on all transparent switches    : true
```

```
Copy running-config to startup-config : true

----------------------------------------

VLAN Port Assignment Parameters

VLAN Name: Test
VLAN Index: 912

Operation: Assign the VLAN to selected port(s)

Port : Fa4/28
Device: 10.77.209.43
Device Address: 10.77.209.43

----------------------------------------

VLAN Trunk Configuration Parameters

VLAN Name: Test
VLAN Index: 912

Operation: Disallow VLAN on selected Trunk(s)

Trunk: 10.77.209.52:2/1 => 10.77.209.61:2/25
Trunk: 10.77.210.211#2:Gi0/2 => 10.77.210.204:Gi1/0/24
```

Review the Summary, and click **Finish** to create the new VLAN, or click **Back** to modify the Disallow VLAN on Trunks page, or click **Cancel** to exit.

Deleting VLANs

You can delete the VLANs configured on the devices in your network. The VLAN Configuration wizard directs you to delete a VLAN.

Step 1 Select **Configuration > Workflows > VLAN > Delete VLAN**.

The VLAN Configuration page appears.

Step 2 Select devices or entities from the VLAN Configuration page.

For more details on selecting the devices, see Selecting Devices or Entities.

Step 3 Click **Delete**.

The Select VLAN to Delete page appears.

Table 10-6 describes the fields in the Select a VLAN to Delete dialog box.

Table 10-6 Select a VLAN to Delete Page Field Description

Field	Description
Copy Running Config to Start-up Config	Check the checkbox to copy the running configuration to start-up configuration.
Delete on all Transparent Switches	Check the checkbox to delete VLANs on all transparent switches. If you have created VLANs by checking Create on all transparent switches, it is mandatory that you check Delete on all Transparent Switches option to delete the VLANs created in VTP Domains.
Filter Source	Select the Filter type of the source: • VLAN • VLAN Name • Domain Name Or enter * or leave the field blank and click **Filter** to get all the records.
Select	Select the radio button corresponding to the VLAN you want to delete.
VLAN ID	Index of the VLAN.
VLAN Name	Name of the VLAN.
Domain Name	Name of the domain in which the VLAN belongs to.

Step 4 Click any of the following:

- **Next** to continue.

  The Move Affected Ports to New VLAN page appears. For more details, see Moving Affected Ports to New VLAN.

- **Cancel** to exit.

  The VLAN configuration appears.

- **Finish** to save changes.

  The selected VLANs are deleted from the devices. The ports in the deleted VLAN are automatically assigned to the default VLAN. The VLAN configuration page appears.

Moving Affected Ports to New VLAN

When you delete a VLAN, any port assigned to that VLAN becomes inactive. Such ports remain associated with the VLAN (and thus inactive), until you assign them to a new VLAN. You can move affected ports to a new VLAN using LMS.

You can move the ports in the VLAN you want to delete, to a new VLAN, only after you select the VLAN you want to delete. For more details on selecting a VLAN to delete, see Deleting VLANs.

To move affected ports to a new VLAN:

Step 1 Select **Configuration > Workflows > VLAN > Configure VLAN**.

The VLAN Configuration page appears.

Step 2 Select devices or entities from the VLAN Configuration page.

For more details on selecting the devices, see Selecting Devices or Entities.

Step 3 Click **Delete**.

The Select VLAN to Delete page appears.

Step 4 Select the radio button corresponding to the VLAN you want to delete and click **Next**.

The Move Affected Ports to New VLAN appears.

Table 10-7 describes the fields in the Move Affected Ports to new VLAN page.

Table 10-7 Move Affected Ports to New VLAN Page Field Description

Field	Description
Port	Affected port in the VLAN.
Device Name	Name of the device to which the port belongs to.
Device Address	IP address of the device.
Port Status	Status of the port.
Connected To	End Host, Network Device

Step 5 Select the new VLAN from the Move affected ports to new VLAN drop-down menu.

If you do not select any VLAN, the affected ports are moved to the default VLAN—VLAN 1.

Step 6 Click any of the following:

- **Next** to continue.

  The VLAN Deletion Summary page appears. For more details, see Understanding VLAN Deletion Summary.

- **Back** to modify the Select VLAN to Delete page.
- **Cancel** to exit.

  The VLAN configuration appears.

- **Finish** to save changes.

  The selected VLANs are deleted from the devices. The ports in the deleted VLAN are assigned to the VLANs selected by you. The VLAN configuration appears.

Understanding VLAN Deletion Summary

The VLAN Deletion Summary page summarizes the operations that you performed through the VLAN Configuration wizard to delete the VLAN. The Summary provides the following information:

- **VLAN Deletion**—Lists the domain name, name of the VLAN that is deleted, and the VLAN ID.
- **Operation: Move the affected Ports to another VLAN**—Lists the name and ID of the new VLAN to which the ports have been moved, and lists the details of the ports including the name and IP address of the device.

Example:

```
VLAN Deletion:
==================

VLAN Domain       :DMZ_10.77.209.43(T)
VLAN Deleted      :VLAN0002
VLANId            : 2

-----------------------------------------

Operation: Move the affected Ports to another VLAN
New VLAN Name :internal VLAN 4
New VLAN Id   :4

Port:Gi1/6
Device :172.20.118.182
Device Address :172.20.118.182

-----------------------------------------
```

Review the Summary and click **Finish** to delete the VLAN, or click **Back** to modify the Select VLAN to Delete page, or click **Cancel** to exit.

Creating Ethernet VLANs

You can use Topology Services to create Ethernet VLANs (which is the typical VLAN design). For details, see Ethernet VLANs.

Ethernet VLANs

An Ethernet VLAN is the typical VLAN design. This consists of a logical group of end-stations, independent of physical location on an Ethernet network. Catalyst switches support a port-centric or static VLAN configuration.

All end stations that are connected to ports that belong to the same VLAN, are assigned to the same Ethernet VLAN. For further details see Creating Ethernet VLANs.

Creating Ethernet VLANs

Before you create Ethernet VLANs, you must create a VTP domain in your network.

Your login determines whether you can use this option.

To create Ethernet VLANs in your network:

Step 1 Either:

- Select **Configuration > Topology**.

Or

- Select **Monitor > Monitoring Tools > Topology Services**.

The Topology Services Main Window appears.

Step 2 Select a VTP domain from the Tree View.

Step 3 Select **Tools > VLAN Management > Create > Ethernet** from the menu.

The VLAN Creation wizard appears. For more details, see Creating VLANs.

Configuring Token Ring VLANs

A Token Ring VLAN is a set of rings interconnected through a bridging function. There are two Token Ring VLAN types defined in VTP version 2:

- Token Ring Bridge Relay Function (trBRF)—Domain of interconnected rings formed, using an internal multiport bridge function.
- Token Ring Concentrator Relay Function (trCRF)—Logical ring domains formed by defining groups of ports that have the same ring number.

You can create Token Ring Bridge Relay Function (trBRF) VLANs and Token Ring Concentrator Relay Function (trCRF) VLANs. Multiple trCRFs can be interconnected using a single trBRF.

A trBRF VLAN is a domain of interconnected rings formed using an internal multiport bridge function. A trCRF VLAN is a logical ring domain formed by defining groups of ports that have the same ring number.

This section contains:

Understanding trBRF VLANs

A Token Ring Bridge Relay Function (trBRF) is a logical grouping of trCRFs. The trBRF is used to join different trCRFs. In addition, the trBRF can be extended across a network of switches through high-speed uplinks between the switches to join trCRFs contained in different switches.

A trBRF has two global parameters: a bridge number and a bridge type. The bridge number is used to identify the logical distributed source-route bridge (SRB), which interconnects all logical rings that have the same parent trBRF.

Creating trBRF VLANs

To create Token Ring Bridge Relay Function (trBRF) VLANs in your network.

Step 1 Select a VTP domain from the Tree View.

Step 2 Select **Tools** > **VLAN Management** > **Create** > **Token Ring BRF** from the menu.

See Table 10-8 for details.

Table 10-8 Creating trBRF VLANs Field Descriptions

Field	Description
VTP Domain	Name of VTP domain in which this VLAN will be created.
VLAN Name	Enter a name for the trBRF.
VLAN Index	Topology Services automatically assigns a VLAN index. This number is incremented each time you create a VLAN in this VTP domain. If you want to change the VLAN index, enter a number between 1 and 1024 to identify the VLAN.
Purpose	Enter a word or phrase that describes the purpose of the VLAN.
Description	Describe the contents of the VLAN.
Create VLAN on all Transparent Switches	Check this box to include this VLAN on switches configured as VTP transparent.
BRF Parameters	
Bridge Number	Integer in hexadecimal format. The default is 0xF.
STP Type	Spanning Tree protocol used in the network.

Step 3 Click **Apply**.

Understanding trCRF VLANs

A Token Ring Concentrator Relay Function (trCRF) is a logical grouping of ports. Each trCRF is contained in only one trBRF, which is called its parent. When a port is assigned to the trCRF, only ports on that switch can belong to that trCRF.

As a rule, a trCRF cannot span different switches. This type of trCRF is called an undistributed trCRF.

However, if your switches are connected through Inter-Switch Link (ISL), the Cisco Duplicate Ring Protocol (DRiP) allows two types of trCRFs in which the ports of a single trCRF can be on different switches.

These types of trCRFs are the default and the backup trCRF:

- Default trCRF

  The default trCRF can contain ports that are located on multiple switches. The default trCRF is associated with the default trBRF, which can span switches through ISL.

  Since the default trCRF is the only trCRF that can be associated with the default trBRF, the default trBRF does not perform any bridging functions, but uses source-route switching to forward traffic between the ports of the default trCRF.

- Backup trCRF

  The backup trCRF allows you to configure an alternate route for traffic between undistributed trCRFs located on separate switches that are connected by a trBRF. The backup trCRF is only used if the ISL connection between the switches becomes inactive.

Creating trCRF VLANs

You must configure a Token Ring Bridge Relay Function (trBRF) VLAN before creating the trCRFs that you want associated with the trBRF.

To create Token Ring Concentrator Relay Function (trCRF) VLANs in your network:

Step 1 Select a trBRF from the Tree View.

Step 2 Select **Tools > VLAN Management > Create > Token Ring CRF** from the menu.

For more information, see Table 10-9.

Table 10-9 Creating trCRF VLANs Field Descriptions

Field	Description
VTP Domain	Name of VTP domain in which this VLAN will be created.
trBRF	Name of trBRF to which this trCRF belongs.
Name	Enter a name for the VLAN.
VLAN Index	Topology Services automatically assigns a VLAN index. This number is incremented each time you create a VLAN in this VTP domain. If you want to change the VLAN index, enter a number between 1 and 1024 to identify the VLAN.

Table 10-9 Creating trCRF VLANs Field Descriptions (continued)

Field	Description
Purpose	Enter a word or phrase that describes the purpose of the VLAN.
Description	Describe the contents of the VLAN.
Create VLAN on all Transparent Switches	Check this box to include this VLAN on switches configured as VTP transparent.
Ring Number	Enter an integer between 1 and 0FFFH, or accept the ring number Topology Services creates.
VLAN Bridge Type	Select a bridging mode for this trCRF.
ARE (All Routes Explorer) Hop Count	Enter the ARE hop count. Valid numbers are 1 to 13, and 7 is the default.
STE (Spanning Tree Explorer) Hop Count	Enter the STE hop count. Valid numbers are 1 to 13, and 7 is the default.
Backup CRF	Check this option if this trCRF is going to be the backup trCRF. A backup trCRF will replace the trBRF if the trBRF fails.

Step 3 Click **Apply**.

The LANE Services option is active.

To configure LANE in your network, click **LANE Services**.

Step 4 Click **OK**.

Your changes are saved and the window closes.

Deleting trBRF and trCRF VLANs

You can delete VLANs in your network. If you delete a VLAN with active ports, it disables the active ports in that VLAN.

You can use VLAN Port Assignment application to move any port to another VLAN.

You can delete a token ring Bridge Relay Function (trBRF) only if all token ring Concentrator Relay Functions (trCRFs) within it have been deleted, or if they do not contain any ports.

Deleting a VLAN with an associated ATM-VLAN does not delete the ATM-VLAN. The ATM-VLAN remains intact and appears in the Standalone ATM-VLANs folder for the ATM domain to which it belongs.

Your login determines whether you can use this option.

To delete a VLAN:

Step 1 Select **Config > Topology Services**.

The Topology Services Main Window appears.

Step 2 Select a VLAN that you want to delete, from the Tree View under Managed Domains.

Step 3 Select **Tools > VLAN Management > Delete**.

The domain window appears with a message:

```
The selected VLAN will be deleted if no ports are associated with this VLAN. Do you want
to continue?
```

Step 4 Check the check box **Delete** on all Transparent Switches, if required.

Step 5 Click **Yes** to delete the VLAN or click **No** to exit.

Interpreting VLAN Summary Information

This section contains:

- Displaying VLAN Reports
- Interpreting VLAN Reports

To display summary information about the VLANs in your network:

From Tree View in Topology Services, open a VTP domain and select a VLAN. The Summary information is displayed in the right pane of the Topology services window. See Table 10-10 to interpret this information.

Note Information on Bridge Number and Ring Number are not applicable to Ethernet VLANs.

Table 10-10 VLAN Field Description

Field	Description
Ports	Number of ports in the domain.
Up Ports	Number of active ports in the domain.
ISL Index	Inter-Switch Link (ISL) index of the VLAN.
Port List	
Link	A lightning bolt indicates a port that is connected to a switch.
PortDescription	Description about the port.
PortName	Name of the port.
Device Name	Name of device to which the port belongs.
Device Address	IP address of device to which the port belongs.
Port Status	Whether the port is active, down, dormant, or testing.
isTrunk	If checked, the port is configured as a VLAN trunk.
Association Type	Type of VLAN.
Port Mode	Displays mode of port. For example, PVLAN-Host, Promiscuous, or non PVLAN.

Displaying VLAN Reports

LMS allows you to generate VLAN reports for devices, switch clouds, or VTP domains.

Step 1 Select **Reports > Technology > VLAN**.

The Report Generator page appears.

The left drop-down list displays LMS Reports.

Step 2 Select **VLAN** from Select a Report drop-down list.

The VLAN page appears with the following information. See Table 10-11:

Table 10-11 VLAN Page Field Description

Field	Description
Scheduling	
Run Type	Select a run type from the drop-down list. The following run types are available: Immediate, Once, Daily, Weekly, Monthly. If you select Immediate, the Job Info fields and Scheduling Date will be dimmed. **Note** Launching immediate VLAN reports for more than 500 devices results in an error. You can schedule reports to run for all devices or launch immediate reports for less than 500 devices.
Date	Select the date and time at which you need to generate the report. Format: 20 Apr 2005 at 01 20

Table 10-11 VLAN Page Field Description (continued)

Field	Description
Job Info	
Job Description	Enter a description for this report.
E-mail	Enter the e-mail id to which the report has to be sent.
Report Publish Path	Use the Default Path check box to publish the report at a specific location. If you check the Default Path check box, it publishes the report in the default directory path. If you uncheck the Default Path check box, it allows you to specify a directory path to which the report is published. If the directory path is not specified, then the report will be published to: • For Windows: C:\Progra~1\CSCOpx\VLAN • For Solaris and Soft Appliance: /opt/CSCOpx/VLAN A PDF format of the report (along with HTML and CSV formats) is published to the specified location.
Attachment Option	Check this check box to attach the report as a CSV file. By default a CSV file is sent to the e-mail address specified in the E-Mail ID field. If you check Add Full Report check box, instead of CSV a PDF format of the report will be sent as an attachment to the specified e-mail id. You need to enable the e-mail Attachment check box and specify the Maximum Attachment size in the System Preferences dialog box (Admin > System > System Preferences) to send the report as an e-mail. If the file size exceeds the Maximum Attachment size, the URL link of the report is sent as an e-mail. You can click the URL link to view the report.

Step 3 Click **Submit** to generate the report. The VLAN reports window appears.

Or

Click **Reset** to change the settings.

You can open VLAN reports page from Topology Services.

To open VLAN reports from Topology Services:

Step 1 Either:

- Select **Configuration > Topology**.

Or

- Select **Monitor > Monitoring Tools > Topology Services**.

The Topology Services Main Window appears.

Step 2 Select a view that contains the device, switch cloud, or the VTP Domain for which you want to view the report.

This view is in the Tree View in the Topology Services Main Window.

Step 3 Select **Reports** > **VLAN Report** from the menu.

or

Right-click the VTP Domain or the device, and select **Display View**.

The Network Topology window appears.

Step 4 Select the device or the switch cloud.

Step 5 Right-click and select **VLAN Report** from the popup menu.

or

Select **Reports** > **VLAN Report**.

The VLAN Report window appears.

Interpreting VLAN Reports

The following information is displayed at the top of the report:

- Device Name
- Device IP
- Device Type
- Domain

Table 10-12 describes the fields in VLAN Report.

Table 10-12 VLAN Report Field Description

Field	Description
VLAN ID	VLAN index.
VLAN Name	Name of the VLAN to which the device belongs.
Status	Status of device can be operational or suspended.
VLAN Type	Types of VLANs to which the device is associated. The VLANs can be normal, primary, isolated, community, or two-way community VLANs.
Associated Primary	VLAN ID of the associated primary VLAN.
MTU Size	MTU size for the corresponding VLAN on that device.
Media Type	Explains in which media type the device operates. Device can be in ethernet, FDDI, or inactive.

Understanding Private VLAN

A Private VLAN (PVLAN) is a VLAN that isolates devices at Layer 2 (L2), from other ports within the same broadcast domain or subnet. PVLAN segregates traffic at L2 and converts a broadcast segment into a non-broadcast multi-access segment.

PVLANs can stop L2 connectivity between end stations on a switch without distributing them into different IP subnets, thus preventing wastage of IP addresses.

You can also assign a specific set of ports within a PVLAN, and thus control the connectivity among them. You can configure PVLANs and normal VLANs on the same switch.

This topic contains Types of Private VLAN Ports

Types of Private VLAN Ports

The ports in a private VLAN are categorized as:

- Promiscuous Ports
- PVLAN Host Ports
- PVLAN Trunk Ports

Promiscuous Ports

Promiscuous port communicates with all other interfaces and ports within a PVLAN. Such ports are used to communicate with external routers, local directories, network management devices, backup servers, administrative workstations, etc.

Ports to the routing module in some switches are promiscuous in nature (for example, MSFC).

PVLAN Host Ports

A PVLAN host port is a port connected to a server or an end host that requires Layer 2 (L2) isolation. A host port exists in the PortFast mode and the BPDU Guard feature is enabled on these ports. These ports can be further classified into:

- Isolated Ports
- Community Ports

This depends on the secondary VLAN to which the ports belong.

Isolated Ports

Isolated ports are completely isolated in L2, from other ports in the same PVLAN. These ports cannot receive the broadcasts from other ports within the same PVLAN, but receive broadcasts from promiscuous ports.

Privacy for the VLAN is ensured at L2 level by blocking the traffic to all isolated ports, except the promiscuous ports. Broadcasts from an isolated port is always forwarded to all promiscuous ports.

Community Ports

Community ports communicate among themselves and with their promiscuous ports. These ports are isolated at L2 from all other ports in other communities, or isolated ports within their private VLAN. Broadcasts propagate only between associated community ports and the promiscuous port.

PVLAN Trunk Ports

Private VLAN Trunk ports are similar to Host ports that can carry multiple VLANs. A Trunk port carries the primary VLAN and the secondary VLANs to the neighboring switch. The Trunk port is unaware of PVLAN and will carry PVLAN traffic without any special action.

Using Private VLAN

A Private VLAN has four distinct parts:

- Primary VLAN

  Manages the incoming traffic from the promiscuous port to isolated, community, two-way community ports, and all other promiscuous ports, in the same primary VLAN.

- Isolated VLAN

  Isolated ports use this VLAN to communicate to the promiscuous ports. The traffic from an isolated port is blocked from reaching all adjacent ports within its private VLAN, except for its promiscuous ports.

- Community VLAN

  A group of community ports use this unidirectional VLAN to communicate among themselves and to manage the outgoing traffic through the designated promiscuous ports from the private VLAN.

- Two-way community VLAN

  A group of community ports use this VLAN to communicate among themselves. This bidirectional VLAN manages the incoming and outgoing traffic for community ports and Multilayer Switch Feature Cards (MSFC).

Isolated and community VLANs are called secondary VLANs.

This section explains:

- Creating PVLAN
- Configuring Promiscuous Ports
- Deleting PVLAN

While creating private VLANs, you:

- Must set VTP to **Transparent** or **Off** modes, for VTP version 2.
- Can create PVLAN on primary server, **Transparent** and **Off** modes for VTP version 3.

LMS enables you to:

- Create primary Private VLAN.
- Create isolated, community or two-way community VLANs.
- Associate secondary VLANs to primary VLANs.
- Assign ports to secondary VLANs.
- Configure promiscuous ports.

Creating PVLAN

To create a Private VLAN, you must designate one VLAN as primary and another as either isolated, community, or two-way community VLAN. Then, you can assign additional VLANs as secondary VLANs.

After creating primary and secondary VLANs you must associate the secondary VLANs to the respective primary VLANs.

Creating a private VLAN involves the following steps:

- Creating Primary VLAN
- Creating Secondary VLAN and Associating to Primary VLAN
- Associating Ports to Secondary VLAN

Creating Primary VLAN

You must create primary VLAN before creating any other secondary VLAN.

To create Primary VLANs:

Step 1 Either

- Select **Configuration > Workflows > VLAN > Create Private VLAN**.

  The Create PVLAN page appears.

Or

- Select **Configuration > Topology**.

Or

- Select **Monitor > Monitoring Tools > Topology Services**.

  The Topology Services Main Window appears.

  – Select a VTP domain from the VTP Tree View, under the Managed Domain or Network View.

  – Select **Tools > PVLAN Management > Create**.

  The Create PVLAN page appears.

Step 2 Select the devices using the Device Selector or the Domain Selector.

For more details, see Step 2 of Selecting Devices or Entities.

Step 3 Select **Primary** from the Private VLAN Type drop-down list.

The Get Primary VLANs tab and the Associated Primary VLAN field is disabled.

Step 4 Enter a name for the VLAN in the VLAN Name field.

Step 5 Enter the VLAN index number for the new Primary VLAN, in the VLAN Index field.

Step 6 Check the check boxes as required:

- To create private VLAN on all transparent switches.
- To copy Running to Startup config for IOS switches.

  The check box for creating private VLANs on all transparent switches, is enabled only when the VLAN contains a device in transparent mode.

Step 7 Click **Create** to create primary PVLAN.

Note You must create primary VLAN before creating any other secondary VLAN.

Creating Secondary VLAN and Associating to Primary VLAN

After creating a primary VLAN, you can create secondary VLANs. Once you create a secondary VLAN, you must associate that to a primary VLAN.

To do this:

Step 1 Either:

- Select **Configuration > Workflows > VLAN > Create Private VLAN**.

  The Create PVLAN page appears.

Or

- Select **Configuration > Topology**.

Or

- Select **Monitor > Monitoring Tools > Topology Services**.

  The Topology Services Main Window appears.

  – Select a VTP domain from the VTP Tree View, under the Managed Domain or Network View.

  – Select **Tools > PVLAN Management > Create**.

  – The Create PVLAN page appears.

Step 2 Select one of the following options from the Private VLAN Type drop-down list:

- Isolated
- Community
- Two-Way Community

Step 3 Select the Associated Primary VLAN.

You can associate a secondary VLAN that you have created to a primary VLAN.

VTP Domain field displays the domain you have chosen.

You may enter the Private VLAN Name that you want to assign.

Step 4 Select the Private VLAN Index.

Step 5 Check the check boxes as required:

- To create private VLAN on all transparent switches.
- To copy Running to Startup config for IOS switches.

  The check box for creating private VLANs on all transparent switches, is enabled only when the VLAN contains a device in transparent mode.

Step 6 Click **Apply** to create PVLAN or click **Cancel** to exit.

Associating Ports to Secondary VLAN

You must associate ports to the secondary VLAN that you have created. You can assign ports to a secondary VLAN as you assign for normal VLANs. For assigning ports to VLANs, see Using VLAN Port Assignment

Configuring Promiscuous Ports

You must associate the promiscuous ports to the PVLANs you have created, to receive traffic from outside the PVLAN.

You can configure only the ports on which Trunking is not enabled.

To configure a Promiscuous Port:

Step 1 Select **Configuration > Workflows > VLAN > Configure Promiscuous Ports**.

The Configure Promiscuous Ports page appears.

Step 2 Select a device or entities from the list using Device Selector or Domain Selector.

Step 3 Click **List Ports**.

The Port List displays the list of ports on the selected devices.

You can filter the list using the Filter or Advanced Filter.

Step 4 Select the ports from the ports listed in the table.

Step 5 Click **Configure**.

The Configure Promiscuous Port window appears.

The Port Details table displays:

- Device Name
- Port Name
- Device IP Address
- IfName

Step 6 Select the VLANs from the list of Available PVLANs.

Step 7 Click **Add** to add to list of **Mapped VLANs**.

Or

Click **Remove** to remove the VLANs from the Map VLANs table.

You can select the Copy Running to Start-up config check-box to copy the running configuration to the start-up configuration.

Step 8 Click **Apply** to configure.

Deleting PVLAN

To delete PVLAN:

Step 1 Select **Configuration > Workflows > VLAN > Delete Private VLAN**.

The Delete PVLAN page appears.

Step 2 Select a device or entities from the list using Device Selector or Domain Selector.

Step 3 Click **List PVLANs** to see a list of PVLANs. See Table 10-13.

Table 10-13 Fields in PVLAN List

Field	Description
PVLAN List	
Filter	You can select any of the following filter criteria: • PVLAN Index • PVLAN Name • PVLAN Type • Associated Primary • Domain Enter the filter string, then click **Filter**.
PVLAN Index	Index value of the PVLAN.
PVLAN Name	Name of the PVLAN.
PVLAN Type	Type of PVLAN. Values are: Primary, Secondary, Community
Associated Primary	Name of the Associated Primary VLAN.
Domain	Domain to which the VLAN belongs to.

Step 4 Select the check box corresponding to the PVLAN you want to delete.

To select all, select the check-box in the table heading.

Step 5 Click **Delete**.

Understanding Inter-VLAN Routing

Inter-VLAN Routing enables to route the traffic between different VLANs. This feature is required when an end station wants to communicate with another end station in a different VLAN. Devices within a VLAN can communicate with one another without the help of a router.

On the contrary, devices in separate VLANs require a routing device to communicate with one another. Network devices in different VLANs cannot communicate with one another without a router to route the traffic between the VLANs.

In most of the network environments, VLANs will be associated with individual networks or subnetworks. In a switched network, VLANs segregate devices into different collision domains and Layer 3 (L3) subnets.

Configuring VLANs for inter-VLAN routing helps to control the size of the broadcast domain and to keep local traffic local. You can configure one or more routers to route traffic in the network.

Layer 2 switches require a L3 routing device (either external to the switch or in another module on the same chassis).

The new L3 Switches accommodate routing capabilities. The router or the switch receives a packet, determines the VLAN to which it belongs, and sends the packet to the appropriate port on the other VLAN.

Using Inter-VLAN Routing

Configuring Inter-VLAN Routing

LMS supports Inter-VLAN Routing configuration on devices like MSFC, RSM, and external routers with IPv4.

Prerequisite for configuring Inter-VLAN Routing

Configuration Functionality in LMS is a prerequisite for configuring Inter-VLAN Routing.

If you want to configure Inter-VLAN Routing on a device:

- LMS must manage the devices.
- The device must have the same device name when managed by LMS.

See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for more details on how to manage devices.

This section contains:

- Configuring Inter-VLAN Routing on RSM, MSFC, L2/L3 Devices
- Configuring Inter-VLAN Routing on External Routers

Configuring Inter-VLAN Routing on RSM, MSFC, L2/L3 Devices

To configure Inter-VLAN Routing on a VLAN interface:

Step 1 Either:

- Select **Configuration** > **Topology**.

Or

- Select **Monitor** > **Monitoring Tools** > **Topology Services**.

The Topology Services Main Window appears.

Step 2 Select a device from the Topology Services Tree View, under the Network Views.

Step 3 Right-click the device and select **Config Inter-VLAN Routing** from the popup menu.

The Configure Inter-VLAN Routing window appears. This window displays the Device Name and the Device IP of the selected device.

Step 4 Select a device interface from Device interface configuration list.

Step 5 Click **Edit** to edit an existing VLAN configuration.

Or

Click **New** to configure Inter-VLAN Routing for a new VLAN interface.

You can edit IP Address, Admin Status, and Subnet Mask. See Table 10-14.

Table 10-14 Configuring Inter-VLAN Routing Field Descriptions

Field	Description
VLAN Interface[1]	Enter the VLAN interface.
IP Address	Enter the IP address for the interface
Subnet Mask	Enter the subnet mask address.
Admin Status	Select the Admin status: • Up • Down

1. You can enter the VLAN interface name to create a new interface. You cannot edit an existing VLAN interface.

You can also delete a Device Interface from the list of Interfaces for which you do not want to configure Inter-VLAN Routing.

Step 6 Click **Move to Interface Set**.

If you want to edit the configuration details again:

a. Select the VLAN interface from the Interface Set.

b. Click **Delete from Interface Set**

c. Repeat the steps from Step 4.

Step 7 Click **Apply**.

You can configure Inter-VLAN Routing for more than one VLAN interface, at a time.

Inter-VLAN Routing is configured for all the VLAN interfaces in Interface Set.

Configuring Inter-VLAN Routing on External Routers

To configure Inter-VLAN Routing on a VLAN interface of an external router:

Step 1 Either:

- Select **Configuration > Topology**.

Or

- Select **Monitor > Monitoring Tools > Topology Services**.

The Topology Services Main Window appears.

Step 2 Select a device from the Topology Services Tree View, under the Network Views.

Step 3 Right-click the device and select **Config Inter-VLAN Routing** from the popup menu.

The Configure Inter-VLAN Routing window appears.

Step 4 Select a device interface from Device interface configuration list.

Step 5 Click **Edit** to edit an existing VLAN configuration.

Or

Click **New** to configure Inter-VLAN Routing for a new VLAN interface.

You can edit IP Address, Admin Status, Encapsulation, and Subnet Mask. See Table 10-15

Table 10-15 Configuring Inter-VLAN Routing Field Descriptions

Field	Description
VLAN Interface[1]	Enter the VLAN interface.
IP Address	Enter the IP address for the interface.
Sub-Interface ID	Enter the ID for the sub-interface.
Admin Status	Select the Admin status: • Up • Down

Table 10-15 Configuring Inter-VLAN Routing Field Descriptions (continued)

Field	Description
Encapsulation	Select the encapsulation: • dot1Q • ISL
Subnet Mask	Enter the subnet mask address.

1. You can enter the VLAN interface name to create a new interface. You cannot edit an existing VLAN interface.

You can also delete a device interface from the list of interfaces for which you do not want to configure Inter-VLAN Routing.

Step 6 Click **Move to Interface Set**.

If you want to edit the configuration details again:

a. Select the VLAN interface from the Interface Set.

b. Click **Delete from Interface Set**

c. Repeat the steps from Step 2.

Step 7 Click **Apply**.

You can configure Inter-VLAN Routing for more than one VLAN interface, at a time.

Inter-VLAN Routing is configured for all VLAN interfaces in the Interface Set.

VLAN Trunking Protocol

VLAN Trunking Protocol (VTP) is a Layer 2 multicast messaging protocol that maps VLANs across all media types and VLAN tagging methods between switches. In this way it maintains the VLAN configuration consistency throughout a network.

VTP reduces the effort in adding, deleting, or renaming a VLAN at each switch, when the VLAN extends to other switches in the network.

VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

With VTP, you can make configuration changes centrally on one switch and have those changes automatically communicated to all the other switches in the network.

The major function of VTP is to distribute VLAN information. You must configure VTP before you configure any VLAN.

Using VTP, each switch in server mode displays the following:

- Management domain on the Trunk ports
- Configuration revision number
- VLANs and their specific parameters.

For more details on VLAN, see Understanding Virtual LAN (VLAN), and for VTP Domains, seeVTP Domains.

This topic contains:

VTP Domains

A VTP domain is made up of one or more interconnected devices that share the same VTP domain name. A switch can be configured to be in only one VTP domain, and each VLAN has a name that is unique within a management domain.

Typically, you use a VTP domain to ease administrative control of your network or to account for physical boundaries within your network. However, you can set up as many or as few VTP domains as are appropriate for your administrative needs.

Consider that VTP is transmitted on all Trunk connections, including ISL, IEEE 802.1Q, 802.10, and LANE.

VTP Domains display and monitor the details of the VLANs in your network. Sometimes includes special cases labeled NULL or NO_VTP.

- NULL—Lists devices that are in transparent mode and that support VTP, but do not have configured domain names. Each of these devices is identified in the list by its IP address.
- NO_VTP—Lists devices that do not support VTP. Each of these devices is identified in the list by its IP address.

However, devices which do not support VTP but support VLANs (for example, Catalyst 2900XL Standard Edition switches) are placed in the NO_VTP domain.

The devices that do not support VLANs and VTP (for example, Catalyst 1900 Standard Edition switches) are placed in the domain category of the neighbor device.

Components of VTP Domains

Within a VTP domain, you can configure switches as follows:

- Server—VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over Trunk links. VTP server is the default mode.
- Client—VTP clients operate in the same way as VTP servers. However, you cannot create, change, or delete VLANs on a VTP client. VTP clients also do not broadcast VTP advertisements like the VTP servers do.
- Transparent—VTP transparent switches do not participate in VTP. A VTP transparent switch does not display its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.

Your VTP domain structure influences the behavior of Topology Services.

Understanding VLAN Trunking Protocol Version 3

VTP version 3 can distribute a list of opaque databases over an administrative domain.

VTP version 3 provides these enhancements to the previous VTP versions:

- Support for extended VLANs.
- Support for creating and advertising private VLANs.
- Support for VLAN instances and MST mapping propagation instances.
- Allows improved server authentication.
- Prevents you from adding the wrong database to a VTP domain.
- Allows interaction with VTP version 1 and VTP version 2.
- Support for configuring VTP version 3 on a per-port basis.
- Enables the network to propagate the VLAN database and other databases.

VTP version 3 is a collection of protocol instances. Each instance handles one database, which is associated with a given feature. VTP version 3 runs multiple instances of the protocol by which it handles the configuration propagation of multiple databases that are independent of one another.

For further details see Support for VTP Version 3.

Support for VTP Version 3

LMS supports the version 3 of VTP. Following are the major features supported in this release:

- Displays Primary server as a subfolder under the parent VTP domain:

  If your network contains devices running VTP version 3, the primary server is displayed as a subfolder under the parent Domain in the VTP Domains. Under Primary server folder, you can find all the server and client modes.

- Supports devices with VTP set to **Off** mode:

  The devices which are set to **Off** mode are supported as for the transparent mode devices. The Tree View displays the **Off** mode devices in subfolder under the parent domain.

- Provides VTP filters:

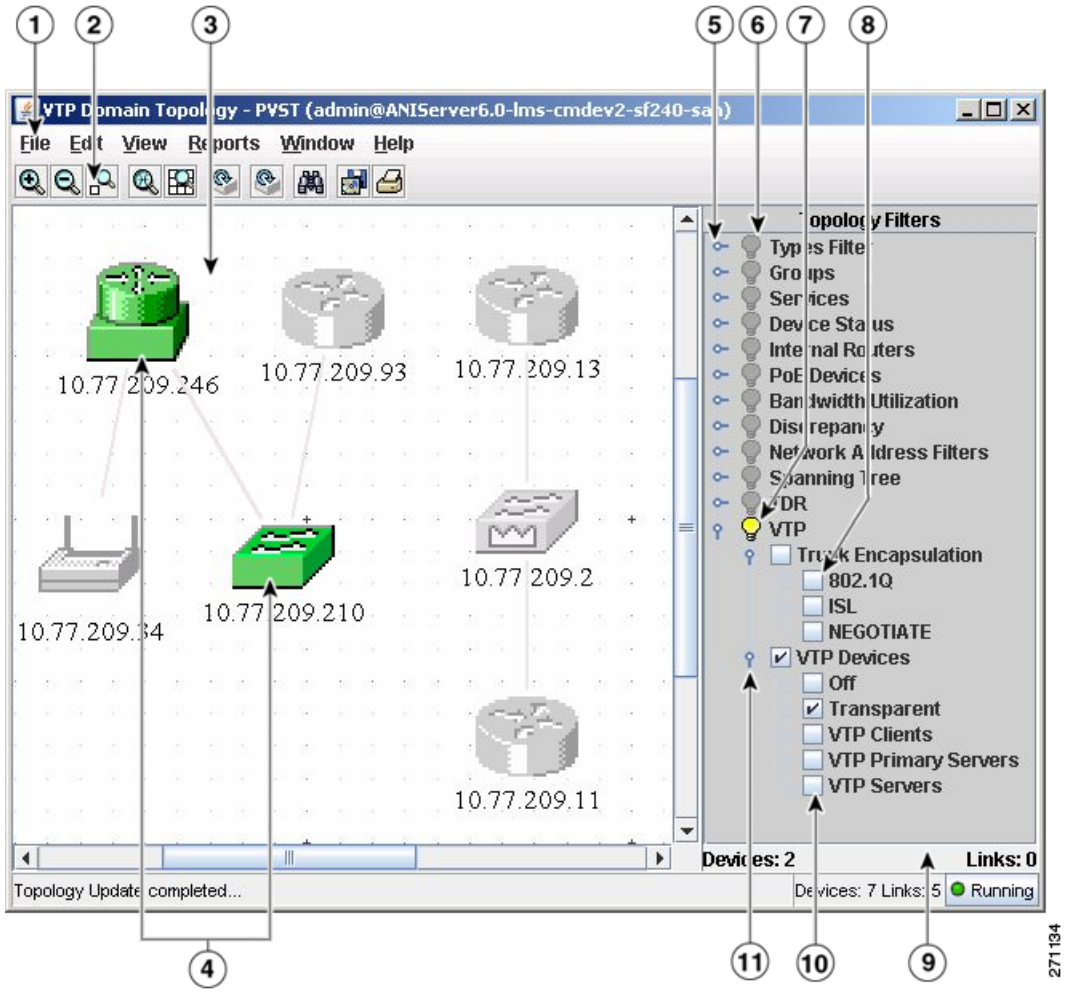
  Topology Filters contains a filter for devices running VTP version 3 in the Network Topology view for the VTP Domains and VTP Views.

  You can enable the filters to view the primary, server, client, transparent, and **Off** mode devices. The **Off** mode devices in VTP version 2 and version 3 domains, are displayed under different subfolders of the parent domain, in the Tree View.

  When you change the configuration through LMS, the **Off** mode devices are considered similar to the **Transparent** mode devices.

  For more details, see Figure 10-1.

Figure 10-1 VTP Filters



1	Menu	**7**	Filter on for VTP devices
2	Toolbar	**8**	Check box dimmed for the filter
3	Topology map	**9**	Topology filter results
4	Filtered devices	**10**	Check box enabled for VTP Transparent devices
5	Filter collapsed	**11**	Expand icon for the filter
6	Filter dimmed		

- Supports creating Private VLANs in VTP version 3 environment.

  You can create a VLAN or PVLAN using a primary server domain or the parent domain. You can create a VLAN or PVLAN only on the Primary server, **Transparent** and **Off** mode devices, in a VTP version 3 environment.

Notes on creating VLAN or PVLAN in VTP version 3 domain using LMS

- You must select the parent VTP domain folder under the VTP domain Tree to create VLAN or PVLAN.
- To create VLAN or PVLAN on all transparent switches in the domain, you can check the check box **Create VLAN on all transparent switches** in the Creating VLAN or PVLAN windows.

  For more details, see Creating Ethernet VLANs and Creating PVLAN.
- You must select the primary domain subfolder under the VTP domain, while creating VLAN and PVLAN on the Primary server mode devices that has clients and secondary servers.
- You must select **Transparent** or **Off** mode subfolders under the parent VTP domain to create VLAN or PVLAN on a single **Transparent** or **Off** mode device respectively.

Using VLAN Trunking Protocol (VTP)

Using VLAN Trunking Protocol (VTP), each switch in server mode advertises its management domain on its Trunk ports, its configuration revision number, and its known VLANs and their specific parameters.

Therefore, a new VLAN must be configured on only one device in the management domain, and the information is automatically learned by all other devices (not in VTP transparent mode) in the same management domain.

After a device learns about a VLAN, it receives all frames on that VLAN from any Trunk port and, if appropriate, forwards them to each of its other Trunk ports.

This topic contains:

Displaying VTP Reports

To display a VTP report for the VTP domains in your network.

Step 1 Either:

- Select **Configuration > Topology**.

Or

- Select **Monitor > Monitoring Tools > Topology Services**.

The Topology Services Main Window appears.

Step 2 Select a VTP domain under the VTP views for which you want to view the report. This view is in the Tree View in the Topology Services Main Window.

The VTP Report, which is the Summary view, appears.

Interpreting VTP Reports

See Table 10-16 to interpret the fields shown in the VT Reports Summary view.

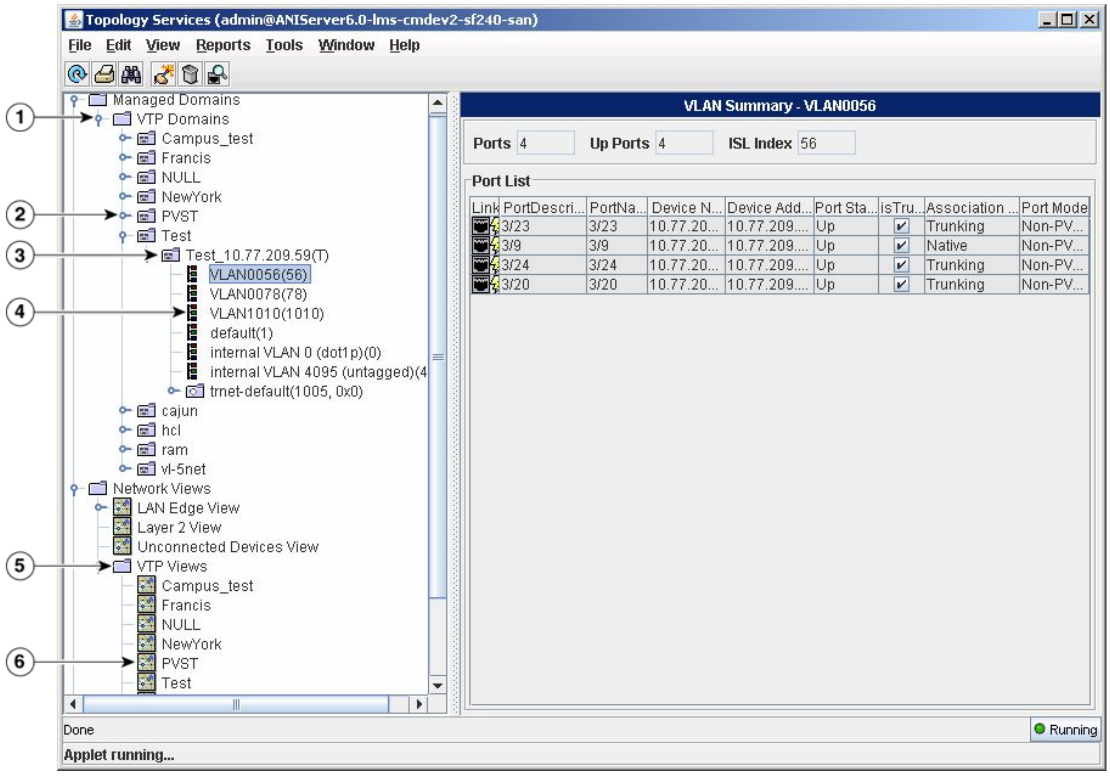
Table 10-16 Field Description for VTP Report

Field	Description
Link	A lightning bolt indicates a port that is linked to a switch.
Port	Number of ports in the domain.
IfName	Interface Name.
Device Name	Name of the device to which the port belongs.
Device Address	Address of the device to which the port belongs.
PortStatus	Displays the status of the port, whether the port is active or dormant.
isTrunk	If the box is checked, the port is configured as a VLAN Trunk.
VLAN	Name of the VLAN.
Association Type	Type of VLAN
Port Mode	Displays the mode of the port. For example, PVLAN-Host, Promiscuous, or a non-PVLAN.

Using VTP Views

VTP Views shows devices that participate in VTP domains. VTP Views also shows the non-VTP devices connected directly to the VTP domain. See Figure 10-2

Figure 10-2 VTP Tree View



1	VTP domain in the Topology Tree View	**4**	VLANs under the Transparent switch mode
2	Parent VTP domain	**5**	VTP Views under the Network View
3	Switch in Transparent mode	**6**	Parent VTP domain under VTP views

Use the VTP views to:

- Display Device Attributes
- Display Port Attributes
- Display Link Attributes
- Display information about multi-layer switching (MLS) devices in your network.

Understanding Trunking

A Trunk is a point-to-point link carrying traffic for several VLANs, and are typically used to connect switches. Instead of configuring several access links to carry multi-VLAN traffic, its economical to do it with a single trunk link.

Trunking is hence a type of configuration on an interface which allows VLANs to span the entire network, instead of just one switch. The Trunked interface that connects to another network device is allowed to pass traffic for multiple VLANs, instead of only one VLAN as in a non-Trunked interface on a switch.

This topic contains:

Trunking Considerations

While using a Trunk, consider the following:

- VLANs are local database of a switch. VLAN information is not passed between switches.
- Trunk links provide VLAN identification for frames traveling between switches.
- You can use either of the two Ethernet Trunking mechanisms: ISL and IEEE 802.1Q.
- Trunks carry traffic from all VLANs to and from the switch by default. However, they can be configured to carry only specified VLAN traffic too.
- Trunk links must be configured to allow Trunking on each end of the link.

Dynamic Trunking Protocol (DTP)

Dynamic Trunking Protocol (DTP) is a Cisco proprietary protocol. Trunk negotiation is managed by the DTP on a link between two devices. DTP is also used for negotiating the type of Trunking encapsulation to be used.

Dynamic Trunking is the ability to negotiate the Trunking method with the other device, and DTP is a point-to-point protocol that supports auto-negotiation of both ISL and 802.1Q Trunks. DTP sends the VTP domain name in a DTP packet.

Therefore, if you use DTP, and if the two ends of a link belong to a different VTP domain, the Trunk will not function.

The Catalyst operating system options of **`auto`**, **`desirable`**, and **`on`**, and the IOS options of **`dynamic auto`**, **`dynamic desirable`**, and **`trunk`**, configure a Trunk link using DTP. If one side of the link is configured to Trunk and sends DTP signals, the other side of the link will dynamically begin to Trunk, if the options match correctly.

To enable Trunking and not send any DTP signaling, you can use the option **nonegotiate** for switches that support that function. If you want to disable Trunking completely, you can use the **off** option for a Catalyst operating system switch or the **no switchport mode trunk** command on an IOS switch.

DTP is a second generation Dynamic Inter-Switch Link Protocol (DISL) and allows the Cisco Catalyst devices to negotiate whether to use 802.1Q encapsulation. DISL and DTP do not negotiate Trunking in case of EtherChannel—they only negotiate whether to enable Trunking.

Trunk Encapsulation

The following Trunking encapsulations are available on all Ethernet interfaces:

- Inter-Switch Link (ISL)—A Cisco-proprietary Trunking encapsulation.
- 802.1Q—An industry-standard Trunking encapsulation.

Trunk Characteristics

Table 10-17 shows the DTP signaling and the characteristics of each mode.

Table 10-17 Trunking Mode Characteristics

Trunking Mode	Frames Sent	Description	Final state (local port)
on	YES, periodic	Trunking is active. The interfaces sends DTP signals that actively attempt to convert the link to a Trunk link. The interface becomes a Trunk interface if the neighboring interface is set to **on**, **auto** or **desirable**, and is running DTP. A port that is in **on** mode always tags frames sent out from the port.	Trunking, unconditionally.
auto	YES, periodic	These links will only become Trunk links if they receive a DTP signal from a link that is already Trunking or desires to trunk. This will only form a Trunk if the neighboring interface is set to **on** or **desirable**. This is the default mode for Catalyst operating system switches.	The port will end up in Trunking state only if the neighboring interface wants to.
desirable	YES, periodic	These links would like to become Trunk links and send DTP signals that attempt to initiate a Trunk. They will only become Trunk links if the other side responds to the DTP signal. This will form a Trunk if the neighboring interface is set to **on**, **auto**, or **desirable** and is running DTP. This is the default mode for all Ethernet interfaces.	If the port detects that the neighboring interface is able to Trunk (remote in **on**, **desirable** or **auto** mode), it will end up in Trunking state. Otherwise, it will stay non-Trunking.

Table 10-17 Trunking Mode Characteristics (continued)

Trunking Mode	Frames Sent	Description	Final state (local port)
`nonegotiate`	NO	Sets Trunking on and disables DTP. These will only become Trunks with ports in `on` or `nonegotiate` mode.	Trunking, unconditionally.
`off`	YES	This option sets Trunking and DTP capabilities off. This is usually the recommended setting for any access port since it prevents any dynamic establishments of Trunk links.	Non Trunking, unconditionally.

Encapsulation Types

The encapsulation type allows you to specify whether ISL or 802.1q should be used for Trunking. The parameter is only relevant if the module you are using is able to use both types of encapsulation. The parameter can have three different values as shown in table below.

Encapsulation Type	Description and Trunking
ISL	Sets the port encapsulation to ISL.
802.1Q	Sets the port encapsulation to 802.1q.
negotiate	Only available in **auto** or **desirable** Trunking modes: • If the neighboring interface has encapsulation type set to **negotiate**, the Trunk will eventually be set up with ISL. • If the interface is configured for ISL or 802.1q or only able to use ISL or 802.1q, the Trunking encapsulation used will be the same as the neighboring interface.

Creating Trunk

To create trunk for a port:

Step 1 Select **Configuration > Workflows > VLAN > Create Trunk**.

The Create Trunk page appears.

Step 2 Select the device or domain from the list, and click **Show Links**.

The Available Links pane displays the links for each device that you have selected. Table 10-18 describes the fields in the Available Links pane.

Table 10-18 Available Links Field Description

Field	Description
Filter	Select the filter type and then enter the string. Leave the field blank to display all. You can filter the list based on the Port1, Device1, Port2, or Device2. For example, if you want to see only the trunks on the selected devices which starts with IP address 10.77, select Device1 from the Filter type, then enter 10.77.* in the filter field and click **Filter**.
Port 1	Port of the first device in the link.
Device 1	IP Address (IPv4 or IPv6 Address) of the device to which the port1 belongs to.
Port 2	Port of the second device in the link.
Device 2	IP Address (IPv4 or IPv6 Address) of the device to which the port2 belongs to.

Step 3 Click the radio button corresponding to the link to select link for which you want to create trunk.

Step 4 Click **Create Trunk**.

Or

From Topology Map, right-click the link for which you want to create trunk, and select **Create Trunk** from the popup menu.

The Create Trunk window appears.

Table 10-19 describes the fields in the Create Trunk page.

Table 10-19 Create Trunk Page Field Description

Field	Description
Device Information	
Device	IP addresses of the devices forming the link.
Port	Port numbers of the devices forming the link.
Trunk Settings	
Encapsulation	Select the Encapsulation type for the trunk. LMS supports: Dot1Q, ISL, Negotiate.
Mode	Trunking mode of the port is set to **Desirable**. LMS supports only the **Desirable** mode.
Configure VLANs on Trunk	
Allow Active VLANs	Lists only the active VLANs. 1. Select the VLANs for which you do not want to configure Trunk. 2. Click **Add** to move the VLANs to Disallowed VLANs list.
Disallow Active VLANs	1. Select the VLAN IDs of the VLANs, which must pass through the Trunk. 2. Click **Remove** to move the VLANs to the list of Allowed VLANs.

Table 10-19 Create Trunk Page Field Description (continued)

Field	Description
Configure VLANSs on Trunk Using Ranges	
Allow VLANs	Enter VLAN IDs of the VLANs, which must pass through the Trunk in the range of 1 to 1005 and 1025 to 4094. The other VLANs are not supported for Trunking.
Disallow VLANs	Enter VLAN IDs of the VLANs, which must not pass through the Trunk, in the range of 1 and 4096. If you enter numbers into both fields, the VLAN indexes that you are disallowing will take precedence over VLAN indexes that you are allowing. For example, if you allow 1-1024 and disallow 1-100, VLANs with ISL indexes of 101-1024 will be allowed.

To copy the running configuration to start-up configuration, select Copy Running to Start-up Config check-box .

Step 5 Click **Create** to create the Trunk or click **Close** to exit.

After you click **Create**, it will be idle for 2 minutes to see if the device goes down on setting the port to trunking mode. After 2 minutes, if the creation of trunk is successful, Data Collection for these devices is triggered.

Only after the completion of Data Collection, you can see the newly configured trunk ports in the Modify Trunk Attributes page.

Note If the trunk link is configured in a port that flaps between blocking and non-blocking states due to STP, then the port will be listed in both Create Trunk page and Modify Trunk Attributes page. To know whether the port is trunking or not, enable logging in the device and see the log messages.

Modifying Trunk Attributes

To modify trunk attributes:

Step 1 Select **Configuration > Workflows > VLAN > Modify Trunk Attributes**.

The Modify Trunk Attributes page appears.

Step 2 Select devices from the device list, and click **Show Trunks**.

The trunks configured on the devices are listed in the Trunk List. See Table 10-20.

Table 10-20 Trunk List Field Description

Field	Description
Filter	Select the filter type and then enter the string. Leave the field blank to display all. You can filter the list based on the Port1, Device1, Port2, or Device2. For example, if you want to see only the trunks on the selected devices which starts with IP address 10.77, select Device1 from the Filter type, then enter 10.77.* in the filter field and click **Filter**.
Port 1	Port number of the port of the device at one side in the link that is configured for Trunking.
Device1	IP Address (IPv4 or IPv6 Address) of the device to which the port1 belongs to.
Port2	Port number of the port of the device at the other end of the link that is configured for Trunking.
Device2	IP Address (IPv4 or IPv6 Address) of the device to which the port2 belongs to.

Step 3 Select the radio-buttons corresponding the trunk you want to modify, and click **Modify Trunk**.

The Modify Trunk window appears.

The Device Information pane displays the device IP address and the port number of all the devices you have selected.

Step 4 Select the Trunk Settings

a. Select Encapsulation:

- Dot1Q
- ISL
- Negotiate

b. Mode

Step 5 Configure VLANs on Trunk.

- Allow VLAN(s)—Enter VLAN IDs of the VLANs, which must pass through the Trunk, in a range between 1 to 1005 and 1025 to 4094. The other VLANs are not supported for Trunking. * indicates that the VLANs were previously disallowed.
- Disallow VLAN(s)—Enter VLAN IDs of the VLANs, which must not pass through the Trunk, in a range between 1 and 4096.

Use the Add or Remove buttons to allow or disallow VLANs.

To copy the running configuration to start-up configuration, select Copy Running to Start-up Config check-box.

Step 6 Click **Modify**.

EtherChannel

EtherChannel is a technology that bundles individual Fast Ethernet and Gigabit Ethernet links into a single logical link that would provide higher bandwidth. EtherChannels thus enable you to aggregate up to Gigabit Ethernet connections, providing up to 16 Gbps of bandwidth (in full duplex mode).

The channel is treated as a single logical connection between two switches. If one of the connections fails in the EtherChannel, the other connections will be operating so that the connection is not down.

This topic contains:

Understanding EtherChannel

EtherChannel provides incremental Trunk speeds between Fast Ethernet (FE) and Gigabit Ethernet (GE) by grouping multiple equal–speed ports into a logical port channel. EtherChannel combines multiple FEs up to 800 Mbps or GEs up to 8 Gbps, providing fault-tolerant, high-speed links between switches, routers, and servers.

LMS supports only PAgP, the aggregation protocol. When a user selects a port or link for configuring EtherChannel, the user is prompted with all available ports that can participate in the channel (Ports that are directly connected between devices).

Admin Group ID attribute for each port is also provided under group attribute. User can change them accordingly to choose which ports need to aggregate into a channel.

All ports that have same group value will participate in channel. LMS supports only the **Desirable** mode for EtherChannel configuration.

LMS does not support EtherChannel configuration between a switch and router.

Using EtherChannel

LMS allows you to:

- Aggregate multiple links between switches into one or more EtherChannels.
- Configure frame distribution parameters for EtherChannel load balancing.

Configuring EtherChannel

To configure EtherChannel:

Step 1 Either:

- Select **Configuration > Topology**.

Or

- Select **Monitor > Monitoring Tools > Topology Services**.

The Topology Services Main Window appears.

Step 2 Select a view that contains the devices for which you want to configure EtherChannel.

This view is in the Tree View in the Topology Services Main Window.

Step 3 Right-click the view and select **Display View** from the popup menu.

The Network Topology View window appears.

Step 4 From the Network Topology View select the link on which you want to configure EtherChannel.

Step 5 Right-click the link and select **Configure EtherChannel**.

The EtherChannel Configuration window appears.

Protocol field displays PAgP. Port Aggregation Protocol (PAgP) is the Protocol that is supported for configuring EtherChannel.

Step 6 Select one of the Distribution Protocols from the drop-down menu:

- ip
- mac
- port
- leave default

  Select **leave default** when you do not want to configure distribution protocols.

The Channel Mode field displays the mode of the port.

LMS supports only the **Desirable** mode for EtherChannel configuration.

Step 7 Select one of these Distribution Address Types from the drop-down menu:

- source
- destination
- both
- leave default

  Select **leave default** when you do not want to configure distribution address type.

Step 8 Select the link for which you want to configure EtherChannel.

Step 9 Click **Copy Running to StartUp config for IOS switches, if required.**

Step 10 Click **Apply** to continue or click **Close** to exit.

VLAN Port Assignment

VLAN Port Assignment is an application that displays device, port, and related VLAN information for an associated VTP domain in a tabular format and helps you manage ports on your network's VLANs.

Use VLAN Port Assignment to:

- Assign or move ports to a VLAN.
- View port, device, and Trunk attributes.
- View and find port information in a VTP domain.
- Configure VLANs on a Trunk.
- Show and highlight a selected device or VLAN on a selected VTP domain.

Note Assigning ports to VLANs cannot be done for more than 100 devices at a time, since it results in memory issues. Do VLAN port assignment for 100 devices at a time.

This topic contains the following sections:

- Understanding VLAN Port Assignment
- Starting VLAN Port Assignment
- Using VLAN Port Assignment

Prior to using VLAN Port Assignment, you should understand the concepts of VLANs and VTP domains. For more details on this, see:

- Understanding Virtual LAN (VLAN)
- VTP Domains

Understanding VLAN Port Assignment

To enable end-user ports to participate in a specific VLAN, you must first assign the ports. You assign ports to specified VLANs. The VLANs allow the ports to share the same broadcasts.

Ports that are not assigned to the VLAN cannot share these broadcasts. For more information about VLANs, see Understanding Virtual LAN (VLAN).

For VLAN Port Assignment to work correctly, LMS must discover the network. LMS requires a properly configured network to complete network discovery.

VLAN Port Assignment queries the ANI database based on criteria you enter.

After you submit the query, VLAN Port Assignment displays the device, port, and related VLAN information for an associated VTP domain. This is displayed in a tabular format.

You can use VLAN Port Assignment to:

- View and find port information in a VTP domain
- View port, device, and Trunk Attributes
- Show and highlight a selected device or VLAN in the VTP domain view

Starting VLAN Port Assignment

To start VLAN Port Assignment:

Step 1 Verify that your network is set up properly.

Step 2 Verify that the LMS server is set up properly and running.

Step 3 Select **Configuration > Workflows > VLAN > Configure Port Assignment**.

If you are prompted to install the Java plug-in, you can download and install the plug-in using the displayed installation screens. The next time you start the application, it will automatically use the plug-in.

Using VLAN Port Assignment

This section provides information to assign ports to VLAN.

To assign ports to a VLAN:

Step 1 Select **Configuration > Workflows > VLAN > Configure Port Assignment**.

The VLAN Port Assignment page appears.

Step 2 Select device or domain from the list using Device Selector or Domain Selector.

Step 3 Click **List Ports**.

A list of ports in the selected devices or entities appears under the Port List. See Table 10-21 for the Port List :

Table 10-21 Port List Field Description

Field	Description
Filter	• Device Name • Device Address • Link • Port • Port Status • Port Description • VLAN Name • VLAN Index • Association Type Enter the filter string, and click **Filter** to filter the list based on the inputs. Leave this field blank to list all ports.
Advanced Filter	Click **Advanced Filter** to open Advanced Filter dialog box. Advanced filtering allows you to search ports using more search criteria. For more details on Advanced Filter, see Advanced Filter.
Columns	
Link	Shows whether the port is connected to a switch or not. The value can either be True or False.
Port	Name of the port.
Device Name	Name of the device to which the port belongs to.
Device Address	IP address of the device to which the port belongs to.
VLAN Name	Name of the VLAN to which the port belongs to.
Port Status	Status of the port. Shows whether the port is active or down.
Port Description	Description for the port. Example: Intra-area 0.2.0.0 Resilient link
VLAN Index	Index number of the VLAN to which the port belongs to.
Association Type	Type of Association.

Step 4 Select a VLAN from the **VLAN** drop-down list.

To copy the running configuration to the start-up configuration, select Copy running to start-up config check-box.

Step 5 Click **Assign**.

Usage Scenarios for Managing VLANs

You can use the following scenarios to manage your network using LMS.

Configuring PVLANs in External Demilitarized Zone

Scenario

Web servers and Domain Name Servers (DNS) are connected to a Demilitarized Zone (DMZ) switch. The DMZ switch is configured with the VTP domain name, DMZ, where the switch is in transparent mode running VTP version 2. The servers belong to the same broadcast domain or VLAN.

Understanding the Scenario

This scenario would help you to isolate Layer 2 devices using PVLAN, and ensure that the DMZ servers do not send data across them, while internal and external hosts access these servers.

DMZ servers must be accessible from external clients as well as from the internal network. DMZ servers eventually needs access to some internal resources, and the servers must not send data across. The servers must not initiate traffic from the DMZ switch to the Internet. The DMZ servers reply only to the traffic from the internal resources.

Understanding Concepts

LMS provides an end-to end solution for configuring Private VLANs, the security feature which LMS provides for managing LANs. You can configure PVLANs using LMS.

You can configure PVLANs in scenarios where Demilitarized Zone (DMZ) switches are configured without adhering to the right policies, leading to potential intrusions into your network.

Demilitarized Zone

Demilitarized Zone is a small subnetwork, which lies between a secure internal network, such as a corporate private LAN, and a non secure external network, such as the public Internet. DMZ contains devices like Web servers, FTP servers, SMTP servers and DNS that are accessible to the Internet traffic.

DMZ servers process incoming requests from the Internet, and initiate connections to certain internal servers or other DMZ segments, such as database servers.

DMZ servers must not send data or initiate any connection to the external networks. This shows that the necessary traffic flows on the basis of a trust model; but the model is not adequately enforced in many networks.

This section contains:

Prerequisites

In this scenario, you need the following applications and tools in LMS.

- Topology Services
- PVLAN configuration user interface
- VLAN Port Assignment
- Promiscuous port configuration user interface
- VLAN report

Reproducing Scenario

To set up the scenario you must configure secondary VLAN on the servers, with isolated ports and community ports. The Firewall, the only device within the primary VLAN, must be defined in a primary VLAN with a promiscuous port.

Step 1 Create a primary VLAN: VLAN 100.

Enter VLAN 100 in the Private VLAN Name field to name the primary VLAN. For more details on creating primary VLAN, see Creating Primary VLAN.

Step 2 Create a community VLAN: VLAN 50.

a. Enter VLAN 50 in the Private VLAN Name field.

b. Associate VLAN 50 to the primary VLAN, VLAN 100.

For more details on creating secondary VLAN, see Creating Secondary VLAN and Associating to Primary VLAN.

Step 3 Create an isolated VLAN: VLAN 60.

a. Enter VLAN 60 in the Private VLAN Name field to name the isolated VLAN

b. Associate VLAN 60 to the primary VLAN, VLAN 100.

For more details on creating secondary VLAN, see Creating Secondary VLAN and Associating to Primary VLAN.

Step 4 Assign ports, which are connected to the Web servers, to the community VLAN 50.

Step 5 Assign ports, which are connected to the DNS servers, to the isolated VLAN 60.

Step 6 Configure the port that connects to the Firewall as a promiscuous port and map the secondary VLAN 50 and VLAN 60 to this promiscuous port. For more details, see Configuring Promiscuous Ports.

After you configure the promiscuous port, the secondary VLANs appear in the Mapped VLANs table.

You have configured promiscuous port and mapped both secondary VLANs to the primary VLAN 100.

If you want to map only the community VLAN 60, you must check the configurations, and map the other isolated VLANs.

Check the **Select to Unmap** check box and click **Apply** to unmap the isolated VLAN from primary VLAN. Community VLAN 60 is unmapped from the primary VLAN.

Verifying Configuration

To verify the configuration for this scenario:

Step 1 Either:

- Select Co**nfiguration > Topology**.

Or

- Select **Monitor > Monitoring Tools > Topology Services**.

The Topology Services Main Window appears.

Step 2 From the Tree View in the Topology Services Main window, verify whether the new PVLANs are listed under DMZ VTP domain in transparent mode.

Primary VLAN 100 is listed as a subfolder under the DMZ domain and the secondary VLAN under the Primary VLAN subfolder. Note that the icon for PVLANs is different from the icon for normal VLANs.

Step 3 Generate VLAN Report for DMZ domain.

Step 4 Verify whether the new primary VLAN and secondary VLANs are listed. The associated primary VLAN is also listed for the secondary VLANs.

Step 5 To confirm that the PVLAN configuration is functioning, you can:

a. Run a trace between the Web servers. The resultant traces must be successful.

b. Run a trace between any Web server and the DNS. The resultant trace must fail.

c. Run a trace between the DNS servers.

CHAPTER 11

Configuring Virtual Routing and Forwarding (VRF)

Using LMS, you can perform end-to-end VRF configurations in an enterprise network. You can perform the VRF Configurations using the following configuration workflows:

- Configuring VRF
- Editing VRF
- Extend VRF
- Deleting VRF

You can assign multiple VLANs to a single VRF instance using Edge VLAN Configuration workflow.

To view and manage VRF configuration jobs, see Using VRF Lite Job Browser.

This section also details the following:

- Scalability Limits
- Pre-requisites

Scalability Limits

In an Enterprise network, LMS is tested to support the configuration of 32 VRFs with VRF configuration supported in 550 devices in your network. However, at a given time, you can select up to 20 devices and configure VRF using the Create, Edit and Extend VRF workflow.

Pre-requisites

The pre-requisites to perform VRF configurations are:

1. The device must be managed by LMS.
2. The device must either be L2/L3 or an L3 device
3. The device must have the necessary hardware support. For more information on hardware support, see http://www.cisco.com/en/US/partner/products/sw/cscowork/ps563/products_device_support_tables_list.html

   If the device hardware is not supported then the device will be classified as Other devices
4. If a device does not support MPLS VPN MIB, it is classified as a Capable device.
5. VTP Server must be support MPLS VPN MIB. If the VTP Server does not support MPLS VPN MIB, LMS will not manage VTP Clients.

Configuring VRF

VRF configurations comprises workflows used to create, edit, extend, delete and assign Edge VLAN to VRF. The VRF Create wizard enables you to create new VRF instances on the selected devices.

To navigate through the Configuration workflows, click **Back** or **Next**. To exit the Configuration workflow, click **Cancel**.

This section explains the Device Selector

Device Selector

To configure VRF on the devices, the devices are selected using the Device Selector. The Device Selector in all the configuration workflows displays the devices that satisfy the following condition:

- Layer2/Layer3 devices
- Layer3 devices

To create VRF, the VRF Creation wizard directs you through:

1. Create VRF
2. Interface Mapping to VRF
3. Routing Protocol Configuration
4. Summary of VRFs to be Configured

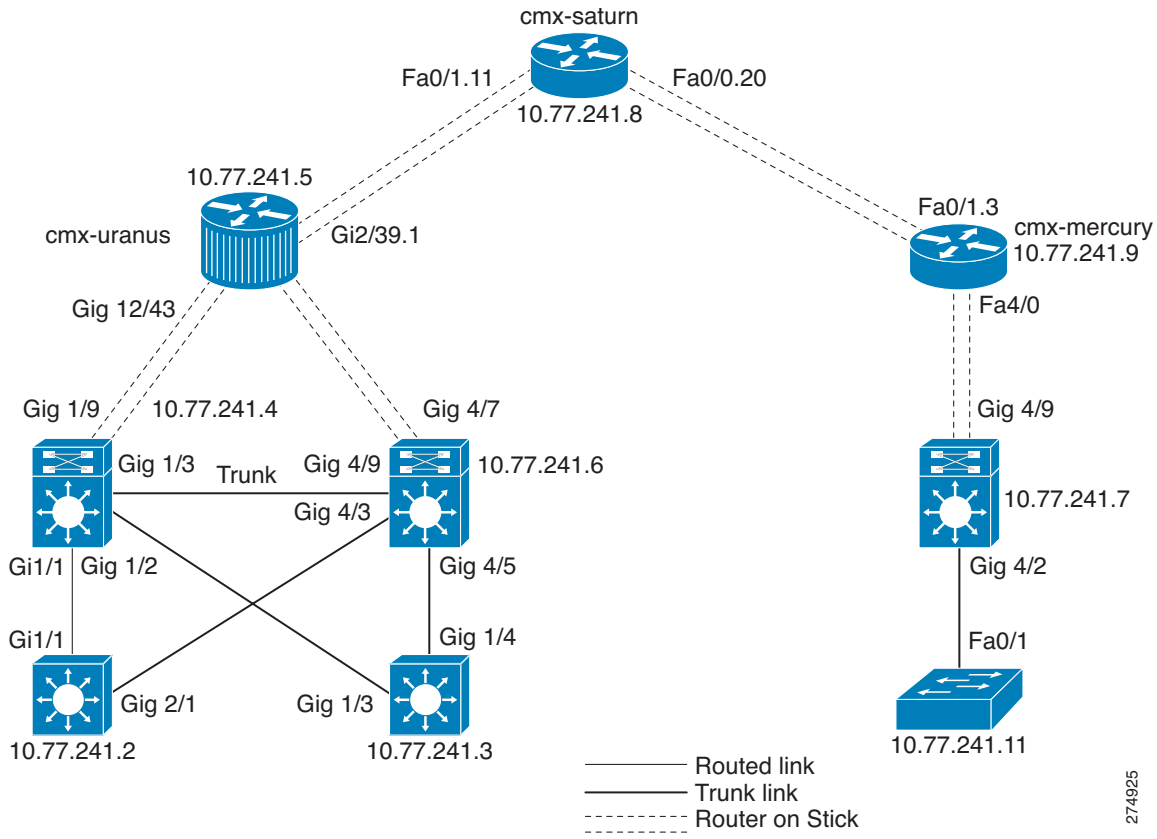
Create VRF

In the Create VRF workflow, you can select the Layer2/Layer3 or Layer 3 devices from the Distribution Layer or the Core Layer. At a given time, you can select up to 20 devices and configure VRF on the selected devices.

After selecting the devices, you can provide following details of VRF: VRF Name, Route Distinguisher and description of VRF that helps you identify the VRF that you have created.

In order to understand the workflows while configuring VRF, consider the topology as shown in Figure 11-1 to demonstrate various stages involved in the VRF creation process. The topology includes devices from Distribution Layer and Core Layer.

Figure 11-1 LMS Topology



Here, the devices selected are 10.77.241.2 and 10.77.241.4. The interface connecting the two devices is a routed interface.

If you select only one device, the VRF creation prompts you to exit the Create VRF wizard, without mapping any interface to the VRF created on the selected device.

To provide end-to-end virtualization for the selected devices, you must virtualize the interfaces connecting devices selected. An interface can be mapped to a VRF in the Interface Mapping to VRF workflow.

To map an interface to the VRF created (virtualize an interface), you must select at least two devices in the VRF creation wizard.

Only users with Network Administrator privileges can create VRFs.

To create VRF:

Step 1 Select **Configuration > Workflows > VRF-lite > Create VRF**.

The Create VRF page appears.

Step 2 Enter the details as mentioned below:

Table 11-1 Settings in Create VRF

Window Element	Description
Device Selector	
Device Selector	The Device Selector displays the devices under the following groups: • All Devices - Represents VRF Supported devices managed by LMS • Device Type Groups - Represents the devices that are grouped as Routers, Switches and Hubs, and Unknown Device Type • User Defined Groups - Represents the devices that are in the user-defined groups. The Device Selector enables you to search and select the devices on which VRF is to be configured. Select the devices using the Device Selector. Check the checkbox to select the device in the groups listed and click **Select**. If you select only one device, the VRF creation wizard is completed without mapping any interface to the VRF created on the selected device. To map an interface to the VRF created, you must select at least two devices in the VRF creation wizard. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector.
VRF Details	
VRF Name	Name of the VRF to be created. Valid values are alphanumeric characters. This field is mandatory.
Route Distinguisher (RD)	Value used to distinguish routes configured in a VRF. Valid values are numeric characters in the format *X:Y*. The valid values for *X* are autonomous numbers. *X* can take values from 1 to 65535 or an IP Address. The valid values for *Y* are numeric values. *Y* can take values from 1 to 65535. For example *X:Y* is in the form 32:66 or 10.10.10.10:22. Note: You must enter a unique value for each VRF that is configured.
Description	Description of VRF to be created. Valid values are alphanumeric characters. With no entry, the default description provided by LMS is “VRF Created by LMS”
Finish	Click **Finish** to create VRF on the selected devices without interface mapping.

Step 3 Click **Next**

The Interface Mapping to VRF window appears. For information on Interface Mapping to VRF, see Interface Mapping to VRF

Interface Mapping to VRF

The Interface Mapping to VRF window displays the Source and the Destination devices selected using Device Selector. The page also displays a list of links in the form of rows.

This section contains:

- Current Mode
- Preferred Virtual Interfaces
- Native VLAN

The Interface Mapping to VRF window is used to map an interface to a VRF. The links displayed are the interfaces connecting a Source device to the Destination device. The mapping is performed from the devices in the Distribution Layer and Core Layer.

Current Mode

The current mode is the existing mode of an interface connecting any two selected devices. The current mode of an interface can be either a Switched or Routed mode.

Preferred Virtual Interfaces

In the Interface Mapping to VRF page, while you are assigning an interface to a VRF, you are prompted to create preferred virtual interfaces on the device. LMS suggests a preferred virtual interface, in scenarios where the current mode cannot be considered for configuring VRF.

The preferred virtual interfaces decide the type of virtual interface to be created, to virtualize an interface that connects the selected devices while you create VRF. The preferred virtual interfaces are based on the family of the selected devices.

The preferred virtual interface type is a part of the metadata XML file. The metadata XML file is used as a repository to store information on the device types and their associated metadata while creating VRF.

LMS has defined the following preferred virtual interfaces for the devices belonging to:

- Cat3k and Cat4k family, SVI is the preferred virtual interface
- Cat 6k and Router category, Sub-interface is the preferred virtual interface

Consider an example where two devices are selected. The virtual interfaces are created based on the current mode.

Note The interfaces that are virtualized using VRF-lite must be Layer 3 interfaces.

IIn the Interface Mapping to VRF page, an interface is virtualized based on the current mode of the interface.

The Interface Configuration modes are mentioned in the Table 11-2

Table 11-2 IInterface Configuration Modes

Current Mode	Trunk is configured	Preferred Mode	LMS Configures
Switched	Yes	SVI	SVI
Switched	Yes	SI	SVI
Switched	No	SVI	Trunk, SVI
Switched	No	SI	Trunk, SVI
Routed [1]	N/A	SVI	Trunk, SVI
Routed [2]	N/A	SI	SI
Routed with Sub-interface configured	N/A	SI	SI. LMS configures with current mode
Routed with Sub-interface configured	N/A	SVI	SI.LMS configures with current mode

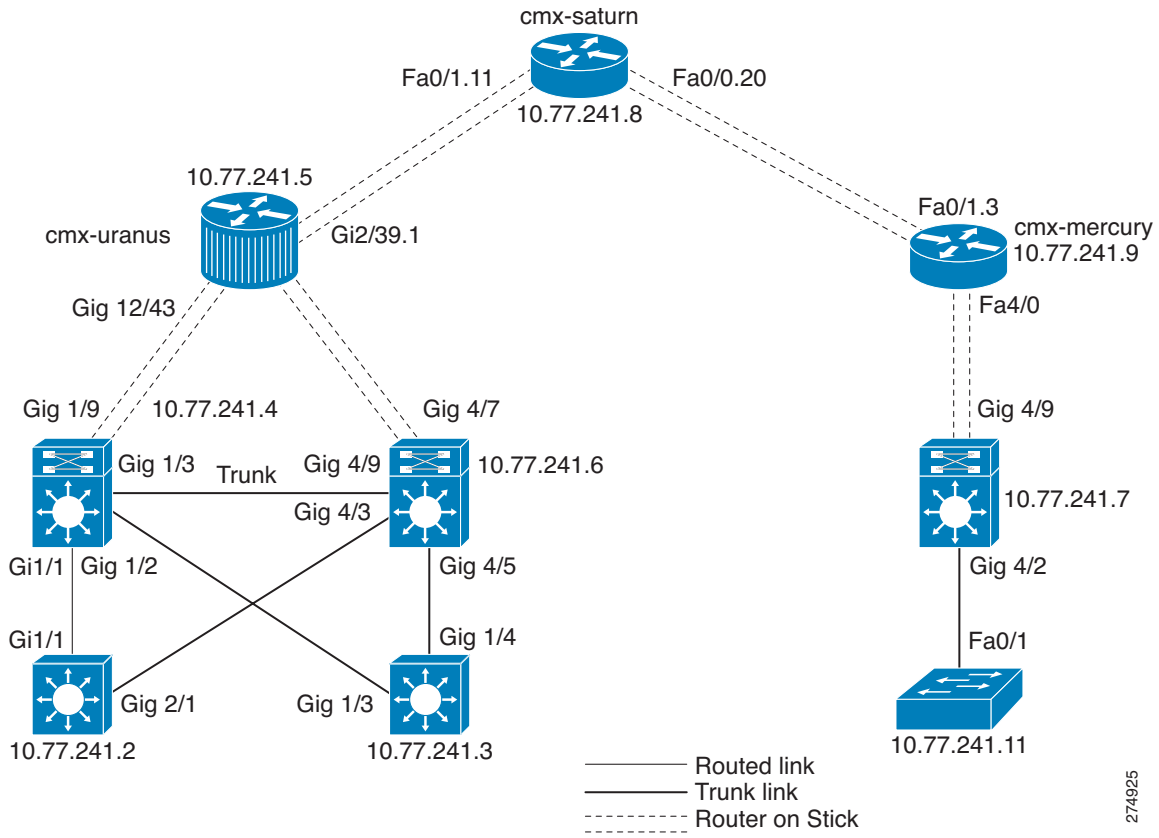
1. Interface is in Routed mode and the Sub-interface is not configured.
2. Interface is in Routed mode and the Sub-interface is not configured.

Native VLAN

In the Interface mapping to VRF page, when you configure the VRF details on an interface, the VRF configurations might affect the global configurations in some scenarios. Therefore, Native VLANs are used for the global configuration traffic.

Consider the source device as 10.77.241.4 with source interface as Gi 1/1 and the destination device as 10.77.241.2 with destination interface as Gi 1/1 as shown in Figure 11-2

Figure 11-2 Native VLAN Configuration



Scenario 1: If both source and destination interfaces are in routed mode, Trunk cannot be configured on the interfaces. To configure Trunk, LMS converts the routed port of the destination interface to switch port. If a free VLAN exists, VNM converts the free VLAN to Native VLAN.

Table 11-3 Scenario 1

Source Interface IP with port mode	Is Trunk	Preferred Mode	Sub-interface configured	Destination Interface IP with port mode	Is Trunk	Preferred Mode	Sub-interface configured
10.77.241.4, Routed	False	SI	Yes	10.77.241.2, Routed	False	SVI	No

Note The IP Address provided for the source and the destination interface must be within the same network. For example: If the source interface IP Address is 10.10.10.2, then the destination interface IP Address must be configured as 10.10.10.3.

Step 1 In the Interface Mapping to VRF window, enter the details as in Table 11-4:

Table 11-4 Interface Mapping to VRF Settings

Window Element	Description
VRF Details	
VRF Name	Name of the VRF to be created.
Source	
Source Device Name	Displays the Source Device name as in Device Credentials and Repository (DCR). Click the arrow icon to view or hide details of the interfaces that are a part of the Source device.
Checkbox	To assign a link to a VRF, check the check box against the interfaces listed under the device name to which they are connected.
Interface	Interface connecting the Source device.
IP Address	Source interface IP Address. Valid IP values are the IPv4 Addresses. This field is blank if the source physical interface is not configured with an IP Address. If you newly configure an IP Address, the corresponding network IP Address must be advertised. You must advertise the IP Address by manually updating the Commands field in the Routing Protocol Configuration page.
Destination	
Device Name	Displays the Destination Device name as entered in Device Credentials and Repository (DCR).
Interface	Interface connecting the Destination device.
IP Address	Destination interface IP Address. Valid IP values are the IPv4 Addresses. If the destination physical interface is not configured with an IP Address, this field is blank. If you newly configure an IP Address, the corresponding network IP Address must be advertised. You must advertise the IP Address by manually updating the Commands field in the Routing Protocol Configuration page.
Subnet Mask	Subnet mask of the interface
is Trunk	Provides the status of the Trunk configuration on the associated physical interface. The following status is displayed: • Not Applicable — In some scenarios, Trunk configuration is not required to configure VRF • True — Trunk is configured on the associated physical interface • Create — Trunk is not configured on the associated physical interface. Click **Create** to create a Trunk.
VLAN ID	VLAN ID on which VRF is configured. VLAN ID is auto-generated. The allowed range is from 1 to 4095. You can edit VLAN ID

Table 11-4 Interface Mapping to VRF Settings (continued)

Window Element	Description
VLAN Name	VLAN Name on which VRF is configured.VLAN Name is auto-generated. You can edit VLAN Name
Finish	Click **Finish** to create VRF on the devices selected and maps the interfaces (connected to the devices) to VRF without deploying the routing protocol configuration details.

Step 2 Click **Next**.

The Routing Protocol Configuration window appears.

For information on Routing Protocol Configuration, see Routing Protocol Configuration.

Warning Messages

In the Create VRF workflow, when you assign an interface to a VRF, in the following scenarios, the Warning messages displayed are:

Table 11-5 Information on Warning Messages

Warning Message	Scenario
One link is not configured as Trunk	Trunk is not configured on the selected physical interfaces displayed in the Interface Mapping to VRF window. You cannot assign VRF to the non-trunk interfaces.
Some of the selected devices are isolated	Reasons for warning about isolated devices are: • Devices selected are not in series: At least one or more devices selected are not connected in series, so the unconnected devices get isolated. You can view these device details in Topology (Layer 2 View). or • Devices with no physical connection: At least one or more selected devices is not physically connected. These devices are isolated device. You can view these device details in Topology (Unconnected View) You cannot assign VRF to interfaces for isolated devices.

Routing Protocol Configuration

The Routing Protocol Configuration window is used to configure the Routing protocol to the selected devices on which VRF is configured.

By default, the Routing Protocol information from the global configuration for OSPF and EIGRP protocols is displayed.

Static Route Configuration

LMS currently supports the following Routing Protocols: OSPF and EIGRP. You can enter the static route configuration using the Configuration Icon in the Routing Protocol Configuration page.

Command Syntax

`ip route vrf` *vrfname Destination IP Address Subnet Mask Router IP Address*

For example:

ip route vrf Red 172.16.30.0 255.255.255.0 172.16.20.2

To configure static route directly using a device, you must enter the command as mentioned in the Command Syntax in the configuration mode.

Step 1 In the Routing Protocol Configuration window, enter the details as given in Table 11-6:

Table 11-6 Routing Protocol Configuration Settings

Window Element	Description
Device Name	Device name to which routing protocol is associated.
IP Address	IP Address of the device.
Routing Protocol	
Routing Protocol	You can configure the routing protocols on the VRF-configured devices. The drop-down list displays the routing protocols running on the selected device. LMS supports following routing protocols: • OSPF • EIGRP Routing Protocols listed are the protocols present in global Configuration details.
View Global	Displays the VRF configuration and the global configuration details of the device name. You cannot edit these details.
Commands	
Commands	Displays the commands used to configure routing protocol configuration on the VRF to be created.
Configuration Icon	Enables you to edit the commands displayed in the Commands field.
Restore Default	Restores Protocol configuration and clear edited Commands details to default global configuration values.
Finish	Enables you to finish the Create VRF workflow without viewing the commands used to deploy the VRF Configurations in the Summary page. Upon clicking finish, a job is created to deploy the VRF Configuration details to the selected devices.

Step 2 Click **Next**

The Summary page appears. For information on Summary, see Summary of VRFs to be Configured.

Summary of VRFs to be Configured

The Summary page summarizes the VRF and the Protocol configuration details to be deployed on the devices selected.

This section contains:

- Sample Summary
- Understanding VRF Configurations for Create VRF

Note Upon successful completion of Create VRF workflow, LMS triggers the Data Collection process. After the Data Collection process is complete, LMS initiates the VRF Collection process.

The Sample Summary summarizes the VRF configuration details on the devices 10.77.241.2 and 10.77.241.4, connected by an interface Gi1/1. For more information, see Figure 11-2.

A sample of the summary is displayed below.

Sample Summary

```
Device:10.77.241.2

ip vrf Green
    description Green VRF
    rd 60:70
vlan 4
    name Vlan_4
vlan 3000
    name VLANforGreenVRF
interface Vlan4
    ip address 20.20.20.1 255.255.255.252
    no shutdown
interface Gi1/1
        switchport trunk native vlan 4
        switchport trunk allowed vlan add 4
        switchport trunk allowed vlan add 3000
        no shutdown
    interface VLAN3000
        ip vrf forwarding GreenVRF
        ip address 20.20.20.1 255.255.255.252
        no shutdown

router eigrp 10
    address-family ipv4 vrf GreenVRF
        autonomous-system 10

        network 10.0.0.0
        network 20.0.0.0
        auto-summary
        eigrp router-id 10.77.241.2
        eigrp stub connected summary
    exit-address-family
Device:10.77.241.4

ip vrf GreenVRF
    description Green VRF
    rd 60:70
interface Gi1/1
    no switchport
    interface Gi1/1.1
```

```
        encapsulation dot1Q 3000
        ip vrf forwarding GreenVRF
        ip address 20.20.20.2 255.255.255.252
        no shutdown

router eigrp 10
    address-family ipv4 vrf GreenVRF
        autonomous-system 10
        network 10.0.0.0
        network 20.0.0.0
        auto-summary
        eigrp router-id 10.77.241.2
        eigrp stub connected summary
    exit-address-family
```

Understanding VRF Configurations for Create VRF

The following VRF configuration details are deployed on the selected devices and corresponding interfaces. The description of the VRF configuration details is given in Table 11-7.

Table 11-7 Create VRF Configuration

Command	Purpose
Device *device name*	Name of the selected device
ip vrf *vrf-name*	Allows you to enter VRF configuration mode and assigns a VRF name
description *vrf-name*	Provides description of the VRF created
rd *route-distinguisher*	Creates a VPN route distinguisher
interface *interface-id*	Allows you to enter the interface configuration mode and specify the Layer 3 interface to be associated with the VRF. The interface can be a routed port or SVI.
encapsulation dot1Q *vlan-identifier*	Allows you to define the encapsulation format as IEEE 802.1Q and specify the VLAN identifier. The VLAN identifier takes values ranging from 1 to 4095.
ip vrf forwarding *vrf-name*	Associates a VRF with an interface or sub-interface
ip address *ip-address mask*	Configure IP Address on an interface or sub-interface.
no shutdown	Enables an interface.
no switchport	Converts Layer 2 switch port interface to a Layer 3 routed physical interface

Step 1 Click **Finish**

A job is created to deploy the VRF configuration details to the selected devices. A confirmation message appears with the Job ID in the Information dialog box.

For example, if you create VRF Red, the message appears, `Successfully created job for confirmation deployment 1051`

Step 2 Click **Job ID** to check status of the Create VRF Configuration Job in the Information dialog box.

Step 3 Click **OK** in the Info dialog box.

To view the VRF configuration job status, go to **Configuration > Job Browsers > VRF Lite**. See Using VRF Lite Job Browser.

Note To exit the VRF Create wizard without deploying the VRF details on the devices selected, click **Cancel**.

Editing VRF

Edit VRF enables you to edit the VRF details on the devices participating in a VRF.

The Edit VRF workflow is used to edit the following details:

- IP Address of the interface connecting the devices that are a part of the selected VRF
- VLAN ID and VLAN Name
- Routing Protocol Configuration
- Exclude an interface that is a part of the selected VRF

Only users with Network Administrator privileges can edit VRF details.

To edit VRF details of the VRF configured devices, the VRF Edit wizard directs you through:

1. Interface Mapping to VRF in Edit VRF
2. Routing Protocol Configuration in Edit VRF
3. Summary of Edit VRF

To edit VRF:

Step 1 Select **Configuration > Workflows > VRF-lite > Edit VRF**.

The Edit VRF page appears. Table 11-8 describes the fields on the Edit VRF page.

Table 11-8 Edit VRF Settings

Window Element	Description
VRF Details	
VRF Name	Shows the list of VRFs as a drop-down list. You can edit the VRF by selecting the VRF from the drop-down list.
Route Distinguisher (RD)	*Display only.* Shows the RD value of the selected VRF in the format *X:Y.* For more information on RD, see Route Distinguisher (RD).
Description	*Display only.* Description of the selected VRF. You cannot edit the description.
Device Selector	

Table 11-8 Edit VRF Settings

Window Element	Description
Device Selector	Device Selector displays pre-selected devices, participating in the selected VRF. The Device Selector displays the devices under the following groups: • All Devices - Represents VRF Configured devices • Device Type Groups - Represents the devices that are grouped as Routers, Switches and Hubs, and Unknown Device Type • User-defined Groups - Represents the devices that are in the user-defined groups. The Device Selector enables you to search and select the devices on which VRF must be configured to edit the VRF functionality. Select the checkbox to select the device in the groups listed and click **Select**. You must select at least two devices to edit the virtualization of the link connecting devices participating in the selected VRF. For more information on the devices listed, see Device Selector.

Note The Device Selector does not display the devices that are not managed by LMS.

Step 2 Click **Next**

The Interface Mapping to VRF window appears.

For information on Interface Mapping to VRF, see Interface Mapping to VRF in Edit VRF.

Consider the devices selected for Edit VRF workflow are: source device 10.77.241.4 with source interface as Gi 1/1 and the destination device as 10.77.241.2 with destination interface as Gi 1/1 as shown in Figure 11-2.

Interface Mapping to VRF in Edit VRF

The Interface Mapping to VRF window displays a list of links connecting the devices, selected in the Edit VRF page, participating in the VRFs to be edited.

The link details are:

- The links displayed, can either be virtualized with the selected VRF or unvirtualized. You can use the Interface checkbox to deselect a link. This unvirtualizes a virtualized link.

  The corresponding negate command is displayed in the Summary of Edit VRF page indicating that the SI or SVI has been removed. You must manually update the negate command for the routing protocols in the Commands in Edit VRF workflow.

- If both interfaces on either side of a link, are virtualized with a VRF, the Interface Mapping to VRF page displays the values of VLAN,Switch Virtual Interfaces (SVIs) or Sub-Interface (SIs) IP address and so on.

- If a link is virtualized only on one side of the interface, the same VLAN is used to virtualize the interface on the other end of the link. LMS application will not use a new VLAN. You can edit the VLAN details in this page.

The Interface Mapping to VRF window is used to map an interface to a VRF. The mapping is performed from the Distribution layer to the Core layer. It also provides information on the Source and the Destination devices associated with a link.

In the Interface Mapping to VRF in Edit VRF page, while assigning an interface to a VRF, LMS suggests preferred virtual interfaces to be created on the device. For more information, see Preferred Virtual Interfaces.

Step 1 In the Interface Mapping to VRF window, enter the details as given in Table 11-9:

Table 11-9 Settings in Interface Mapping to VRF in Edit VRF

Window Element	Description
VRF Details	
VRF Name	*Display only.* Name of the VRF selected.
Source	
Source Device Name	Displays the Source Device name as entered in Device Credentials and Repository (DCR). Click the arrow icon to view or hide SIs or SVIs that are a part of the source device, participating in the VRF selected.
Checkbox	To assign an SI or SVI to a VRF, check the check box against the SVIs or SIs listed under the device name to which they are connected. When you uncheck the checkbox to deselect a link to unvirtualize a virtualized link, the corresponding Negate command appears in the Summary of Edit VRF page. You must manually update the negate command for the routing protocols in the Commands in Edit VRF workflow.
Interface	*Display only.* Shows the SVIs or SIs name in the Source device.
IP Address	If the interface is virtualized with a configured IP Address, it displays an SI or SVI. You can edit the IP Address. Valid IP values are the IPv4 Addresses. This field will be empty if the source physical interface is not configured. If you configure an IP Address newly, you must advertise the corresponding network IP Address by manually updating the Commands in Edit VRF field.
Destination	
Device Name	*Display only.* Shows the Destination Device name as it appears in the Device Credentials and Repository (DCR).
Interface	*Display only.* Shows the name of the SVIs or SIs in the Destination device.
IP Address	If the interface is virtualized with a configured IP Address, it displays an SI or SVI. You can edit the IP Address. Valid IP values are the IPv4 Addresses. This field will be empty if the source physical interface is not configured. If you configure an IP Address newly, you must advertise the corresponding network IP Address by manually updating the Commands in Edit VRF field.
Subnet Mask	Subnet mask of the IP Address of SVI or SI.

Table 11-9 Settings in Interface Mapping to VRF in Edit VRF

Window Element	Description
is Trunk	Provides the status of the Trunk configuration on the associated physical interface. The following status appears: • True — Trunk is configured on the associated physical interface • Create — Trunk is not configured on the associated physical interface. To configure a Trunk, click **Create** hyperlink. A message appears if the Trunk creation fails.
VLAN Name	VLAN Name on which VRF is configured. VLAN Name is auto-generated.
VLAN ID	VLAN ID on which VRF is configured. VLAN ID is auto-generated. You can edit VLAN ID.

Step 2 Click **Next**

The Routing Protocol Configuration window appears.

For information on Routing Protocol Configuration, see Routing Protocol Configuration in Edit VRF.

Routing Protocol Configuration in Edit VRF

The Routing Protocol Configuration window displays details of the configured Routing protocols. These protocols are associated to the individual devices that you selected. VRF is configured on these devices.

The details of the routing protocol running in the global configuration, are also displayed.

Step 1 In the Routing Protocol Configuration window, enter the details as given in Table 11-10

Table 11-10 Routing Protocol Configuration Settings

Window Element	Description	Usage Notes
Device Name	Device name to which routing protocol is associated.	Display only.
IP Address	IP Address of the device.	Display only.
Routing Protocol		

Table 11-10 Routing Protocol Configuration Settings (continued)

Window Element	Description	Usage Notes
Routing Protocol	You can configure the Routing protocols on VRF-configured devices. The drop-down list displays the routing protocols running on the selected device. LMS supports following routing protocols: • OSPF • EIGRP Routing Protocols listed are the protocols in global configuration details.	You can choose the desired routing protocol.
View Global	Displays the global routing protocol configuration details of the device name. You cannot edit these details.	Click **View Global** to view the global configuration details.

Table 11-10 Routing Protocol Configuration Settings (continued)

Window Element	Description	Usage Notes
Commands in Edit VRF		
Commands	Displays the commands used to configure routing protocol configuration on the VRF to be edited.	You cannot enter a value in this field. To edit the command details: Click **Configuration Icon** The newly configured IP Address for SIs or SVIs entered in the Interface Mapping to VRF in Edit VRF page, must be advertised using this field. To edit the command details: 1. Click **Configuration Icon and** enter the IP Address to be advertised. Valid IP values are the IPv4 Addresses. 2. Click the tick mark to save the changes. 3. Click the close mark to close without saving the changes.
Configuration Icon	Enables you to edit the commands displayed in the Commands field.	Click **Configuration Icon** to edit the Commands field details. Or To enter Static Route Configuration, click **Configuration Icon,** delete the commands displayed in the commands field and enter the commands mentioned in the Command Syntax.
Restore Default	Restores the edited Routing Protocol configuration details to the configuration values computed in the Edit VRF workflow.	Click **Restore Default** to restore VRF Configuration details to default Global values.

Step 2 Click **Next**

The Summary page appears.

For information on Summary, see Summary of Edit VRF

Summary of Edit VRF

The Summary page provisions you with the VRF and the Protocol configuration details to be deployed to the selected devices.

This section contains Sample Summary for Edit VRF

Note Upon successful completion of Edit VRF workflow, LMS triggers the Data Collection process. After the Data Collection process is complete, LMS initiates the VRF Collection process.

The Sample Summary summarizes the VRF configuration details on the devices 10.77.241.2 and 10.77.241.4, connected by an interface Gi1/1. For more information, see Figure 11-2.

A sample of the summary is displayed below.

Sample Summary for Edit VRF

```
Device:10.77.241.2

ip vrf Green
    description Green VRF
    rd 60:70
vlan 4
    name Vlan_4
vlan 3000
    name VLANforGreenVRF
interface Vlan4
    ip address 20.20.20.1 255.255.255.252
    no shutdown
interface Gi1/1
        switchport trunk native vlan 4
        switchport trunk allowed vlan add 4
        switchport trunk allowed vlan add 3000
        no shutdown
    interface VLAN3000
        ip vrf forwarding GreenVRF
        ip address 20.20.20.1 255.255.255.252
        no shutdown

router eigrp 10
    address-family ipv4 vrf GreenVRF
        autonomous-system 10

        network 10.0.0.0
        network 20.0.0.0
        auto-summary
        eigrp router-id 10.77.241.2
        eigrp stub connected summary
    exit-address-family
Device:10.77.241.4

ip vrf GreenVRF
    description Green VRF
    rd 60:70
interface Gi1/1
    no switchport
    interface Gi1/1.1
        encapsulation dot1Q 3000
        ip vrf forwarding GreenVRF
        ip address 20.20.20.2 255.255.255.252
        no shutdown
```

```
router eigrp 10
    address-family ipv4 vrf GreenVRF
        autonomous-system 10
        network 10.0.0.0
        network 20.0.0.0
        auto-summary
        eigrp router-id 10.77.241.2
        eigrp stub connected summary
    exit-address-family
```

Understanding VRF Configurations for Edit VRF

The VRF configuration details edited are deployed on the selected devices and corresponding interfaces. To understand the VRF configuration details edited, see Understanding VRF Configurations for Create VRF.

Step 1 Click **Finish**

A job is created to deploy the edited VRF configurations details to the selected devices. A confirmation message appears with the Job ID in the Information dialog box.

For example, if you edit VRF Red, the message appears, `Successfully created job for confirmation deployment. 1053`

Step 2 Click **Job ID** to check status of the Job in the Info dialog box.

Step 3 Click **OK** in the Info dialog box.

To view the VRF configuration job status, go to **Configuration > Job Browsers > VRF Lite**. See Using VRF Lite Job Browser.

Extend VRF

Extend VRF enables you to extend the VRF functionality across the network. You can extend VRF configuration details by selecting the devices that are neighbors to the VRF-configured devices in a network.

Only the following users have privileges to extend VRF details: Network Administrator, System Administrator and Super Admin.

To extend VRF functionality to other devices, the VRF Extend wizard directs you through:

1. Extending VRF
2. Interface Mapping to VRF in Extend VRF
3. Routing Protocol Configuration in Extend VRF
4. Summary of Extend VRF

To extend VRF:

Step 1 Select **Configuration > Workflows > VRF-lite > Extend VRF.**

The Extend VRF page appears. Table 11-11 describes the Extend VRF page.

Table 11-11 Settings in Extend VRF

Window Element	Description	Usage Notes
VRF Details		
VRF Name	Name of the VRF selected.	You can select the VRF from the VRF Name drop-down list.
Route Distinguisher (RD)	Displays the RD value of the VRF entered while creating a VRF. Note: You must enter a unique value for each VRF that is configured. For more information on RD, see Route Distinguisher (RD).	Displays the RD value of the VRF selected in the format *X:Y*. You can edit the RD value. The edited RD value is applied only to the new devices that were added while extending the VRF.
Description	Displays the description of the VRF entered while creating a VRF.	Displays the description of the VRF selected. You can edit the description. The edited description is applied only to the new devices that were added while extending the VRF.

Table 11-11 Settings in Extend VRF (continued)

Window Element	Description	Usage Notes
Device Selector		
Device Selector	Device Selector displays all the devices, except the devices participating in the selected VRF. It does not display any device that is configured with the VRF selected. The Device Selector also displays the devices under the following groups: • All Devices—Devices which are not participating in the selected VRF • Device Type Groups—Devices that are grouped as Routers, Switches and Hubs, and Unknown Device Type • User-defined Groups—Represents the devices that are in the user-defined groups. The Device Selector enables you to search and select the devices on which VRF must be configured to extend the VRF functionality. See *Inventory Management with Cisco Prime LAN Management Solution 4.1* for information on how to use the Device Selector	Select the devices using the Device Selector. Click the checkbox to select the device in the groups listed and click **Select**.

Note The Device Selector does not display the devices that are not managed by LMS.

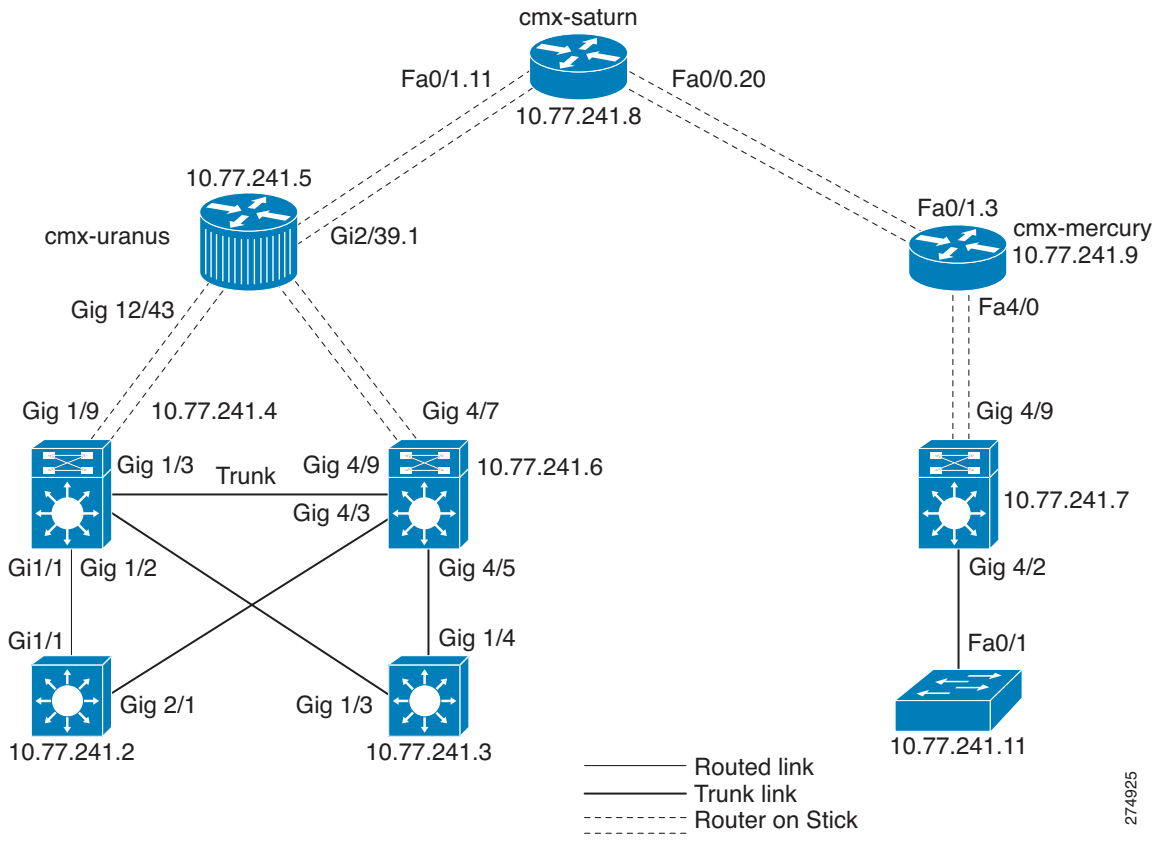
Step 2 Click **Next**

The Interface Mapping to VRF window appears.

For information on Interface Mapping to VRF, see Interface Mapping to VRF in Extend VRF.

In Extend VRF, consider the devices selected are 10.77.241.4 and 10.77.241.6. For more information, see Figure 11-3.

Figure 11-3 Extend VRF workflow



Interface Mapping to VRF in Extend VRF

The Interface Mapping to VRF window displays a list of links that connect the devices. These are the devices that you selected using Device Selector in the Extend VRF window.

The links displayed are:

- Links that connect the devices selected in Device Selector (in Extend VRF page)
- Links that connect the devices selected in Device Selector (in Extend VRF page) and the L2 neighboring VRF-configured device that is not selected in Device Selector (in Extend VRF page)
  - If the links associated with the L2 neighboring device are configured with the selected VRF, only the link is displayed.
  - If the neighbor device is not configured with the selected VRF and it is not selected in Device Selector, the device is not displayed in the Interface Mapping to VRF page.

Note the following about links:

- If both interfaces on either side of a link are not virtualized with a VRF, the Interface Mapping to VRF page displays the values of VLAN, SI or SVI, IP address configured.

- If a link is virtualized only on one side of the interface, the same VLAN is used to virtualize the interface on the other end of the link. LMS will not use a new VLAN. You can edit the VLAN details in this page.

You cannot exit out the extend VRF workflow while it is running by clicking **Finish** in the Interface Mapping to VRF window.

The Interface Mapping to VRF window is used to map an interface to a VRF. The mapping is performed from the Distribution layer to the Core layer. It also provides information on the Source and the Destination devices associated with a link.

In the Interface Mapping to VRF in Extend VRF page, while assigning an interface to a VRF, LMS suggests preferred virtual interfaces to be created on the device. For more information, see Preferred Virtual Interfaces.

Step 1 In the Interface Mapping to VRF window, enter the details as given in Table 11-12:

Table 11-12 Settings in Interface Mapping to VRF in Extend VRF

Window Element	Description	Usage Notes
VRF Details		
VRF Name	Name of the VRF selected.	You cannot edit this field.
Source		
Source Device Name	Displays the Source Device name as entered in Device Credentials and Repository (DCR).	Click the arrow icon to view or hide details of the SIs or SVIs that are a part of the source device and participating in the VRF selected.
Checkbox	Allows you to select or deselect an SVI or SI that must be assigned to a VRF.	• To select, check against the SVIs or SIs listed under the device name to which they are connected. Or • To deselect, uncheck against the SVIs or SIs listed under the device name to which they are connected.
Interface	Switch Virtual Interfaces (SVIs) or Sub-Interface (SIs) name in the source device.	Display only.
IP Address	If the interface is virtualized, with IP Address configured, it displays an SI or SVI. You can edit the IP Address. This field is empty if the source physical interface is not configured. If you newly configure an IP Address, the corresponding network IP Address must be advertised. You must advertise the IP Address by manually updating the Commands in Extend VRF field.	Enter the IP Address. Valid IP values are the IPv4 Addresses.

Table 11-12 Settings in Interface Mapping to VRF in Extend VRF

Window Element	Description	Usage Notes
Destination		
Device Name	Displays the Destination Device name as entered in Device Credentials and Repository (DCR).	Display only.
Interface	Switch Virtual Interfaces (SVIs) or Sub-Interface (SIs) name in the Destination device.	Display only.
IP Address	If the interface is virtualized, with IP Address configured, it displays an SI or SVI. You can edit the IP Address. This field is empty if the source physical interface is not configured. If you newly configure an IP Address, the corresponding network IP Address must be advertised. You must advertise the IP Address by manually updating the Commands in Extend VRF field.	Enter the IP Address. Enter the IP Address of the
Subnet Mask	Subnet mask of IP Address of SVI or SI	Enter the subnet mask
is Trunk	Provides the status of the Trunk configuration on the associated physical interface. The following status is displayed: • True — Trunk is configured on the associated physical interface • Create — Trunk is not configured on the associated physical interface.	To configure Trunk, click **Create** hyperlink. After clicking **Create**, Trunk is created.
VLAN Name	VLAN Name on which VRF is configured.VLAN Name is auto-generated.	You can edit VLAN Name.
VLAN ID	VLAN ID on which VRF is configured.VLAN ID is auto-generated or configured.	You can edit VLAN ID.

Step 2 Click **Next**

The Routing Protocol Configuration window appears.

For information on Routing Protocol Configuration, see Routing Protocol Configuration in Extend VRF.

Routing Protocol Configuration in Extend VRF

The Routing Protocol Configuration window displays details of the configured Routing protocols. These protocols are associated to the individual devices that you selected. VRF is configured on these devices.

Details about the Routing protocol running in the global configuration table are also displayed.

Step 1 In the Routing Protocol Configuration window, enter the details as given in Table 11-6:

Table 11-13 Routing Protocol Configuration Settings

Window Element	Description	Usage Notes
Device Name	Device name to which routing protocol is associated.	Display only.
IP Address	IP Address of the device.	Display only.
Routing Protocol		
Routing Protocol	You can configure the routing protocols on VRF-configured devices. The drop-down list displays the routing protocols running on the device selected. LMS supports following routing protocols: • OSPF • EIGRP Routing Protocols listed are the protocols present in global configuration details.	You can choose the Routing protocol that you want.
View Global	Displays the VRF configuration and the global configuration details of the device name. You cannot edit these details.	Click **View Global** to view the Global Configuration details.
Commands in Extend VRF		
Commands	Displays the commands used to configure routing protocol configuration on the VRF to be extended.	You cannot enter a value in this field. To edit the command details: The newly configured IP Address for SIs or SVIs entered in the Interface Mapping to VRF in Extend VRF page, must be advertised using this field. Valid IP values are the IPv4 Addresses To edit the command details, Click **Configuration Icon and** enter the IP Address to be advertised. After entering the details, click the tick mark to save the changes. Click **Configuration Icon** and click the tick mark to save the changes.

Table 11-13 Routing Protocol Configuration Settings (continued)

Window Element	Description	Usage Notes
Configuration Icon	Enables you to edit the commands displayed in the Commands field.	Click **Configuration Icon** to edit the Commands field details. Or To enter Static Route Configuration, click **Configuration Icon,** delete the commands displayed in the commands field and enter the commands mentioned in the Command Syntax.
Restore Default	Restores Protocol configuration and clears edited Commands details to default Global Configuration values.	Click **Restore Default** to restore VRF Configuration details to default Global values.

Step 2 Click **Next**

The Summary window appears.

For information on Summary, see Summary of Extend VRF

Summary of Extend VRF

The Summary window displays the VRF and the Protocol configuration details to be deployed on the selected devices.

This section contains:

- Sample Summary for Extend VRF
- Understanding VRF Configurations for Extend VRF

Note Upon successful completion of Extend VRF workflow, LMS triggers the Data Collection process. After the Data Collection process is complete, LMS initiates the VRF Collection process.

The Sample Summary summarizes the VRF configuration details on the devices 10.77.241.4 and 10.77.241.6. For more information, see Figure 11-3.

A sample of the summary is displayed below.

Sample Summary for Extend VRF

```
Device:10.77.241.4
vlan 5
    name Vlan_5
interface Gi1/3
        switchport trunk allowed vlan add 5
    interface Vlan5
        ip vrf forwarding GreenVRF
        ip address 5.5.5.1 255.255.255.252
        no shutdown
```

```
router eigrp 10
    address-family ipv4 vrf GreenVRF
        autonomous-system 10

        network 5.0.0.0
        auto-summary
        eigrp router-id 10.77.241.4
        eigrp stub connected summary
    exit-address-family

Device:10.77.241.6

ip vrf GreenVRF
    description Green VRF
    rd 70:80
vlan 5
    name Vlan_5
interface Gi4/9
        switchport trunk allowed vlan add 5
    interface Vlan5
        ip vrf forwarding GreenVRF
        ip address 5.5.5.2 255.255.255.252
        no shutdown

router eigrp 10
    address-family ipv4 vrf GreenVRF
        autonomous-system 10

        network 5.0.0.0
        auto-summary
        eigrp router-id 10.77.241.4
        eigrp stub connected summary
    exit-address-family
```

Understanding VRF Configurations for Extend VRF

To extend VRFs to selected devices and corresponding interfaces, the VRF configuration details are deployed on the selected devices and corresponding interfaces. To understand the VRF configuration details edited, see Understanding VRF Configurations for Create VRF

Step 1 Click **Finish**

A job is created to deploy the VRF configurations details to the selected devices. A confirmation message appears with the Job ID in the Information dialog box.

For example, if you extend VRF Red, the message appears, `Successfully created job for confirmation deployment.1052`

Step 2 Click **Job ID** to check status of the Job in the Info dialog box.

Step 3 Click **OK** in the Information dialog box.

To view the VRF configuration job status, go to **Configuration > Job Browsers > VRF Lite**. See Using VRF Lite Job Browser.

Deleting VRF

Delete VRF workflow is used to delete the VRFs present on your network.

The Delete VRF workflow enables you to:

- Delete VRF from the selected devices
- Delete virtual interfaces that are virtualized by the VRF of the selected device
- Delete virtualized virtual interfaces from the devices, at the other end of the physical interface that connects the selected device.

  For example, Device A with virtual interface (Gig5/1.1) is connected to Device B with virtual interface (Gig4/1.1). (Assume that the virtual interfaces of both devices are virtualized with the selected VRF.)

  If you select Device A using Device Selector, Device B will be on the other end of the physical interface that is connected to Device A. In this case, the virtual interface(Gig5/1.1) on Device A, and virtual interface(Gig4/1.1) on Device B will be deleted.

  You cannot delete Layer2 VLANs using the Delete VRF feature.
- Delete internal VLANs created for Sub-Interfaces (SIs)

The following users have the privilege to delete VRF: Network Administrator and Super Admin. The user privileges mentioned is applicable for local mode only.

To delete VRF:

Step 1 Select **Configuration > Workflows > VRF-lite > Delete VRF**.

The Delete VRF: VRF and Device Selection page appears. Table 11-14 details the Delete VRF: VRF and Device Selection page.

Table 11-14 Delete VRF: VRF and Device Selection

Window Element	Description
VRF Details	
VRF Name	Shows the list of VRFs as a drop-down list. You can delete the VRF by selecting the VRF from the drop-down list.
Route Distinguisher (RD)	*Display only.* Shows the RD value of the selected VRF in the format *X:Y.* For more information on RD, see Route Distinguisher (RD).
Description	*Display only.* Description of the selected VRF. You cannot edit the description.
Device Selector	

Table 11-14 Delete VRF: VRF and Device Selection

Window Element	Description
Device Selector	Device Selector displays VRF-configured devices with selected VRF. The Device Selector displays the devices under the following groups: • All Devices - Represents VRF Configured devices • Device Type Groups - Represents the devices that are grouped as Routers, Switches and Hubs, and Unknown Device Type • User-defined Groups - Represents the devices that are in the user-defined groups. The Device Selector enables you to search and select the devices on which VRF functionality must be deleted. Select the checkbox to select the device in the groups listed. For more information on the devices listed, see Device Selector.

Step 2 Click **Next**

The Summary window appears.

For information on Summary, see Delete VRF - Summary.

Delete VRF - Summary

The Summary window summarizes the commands that will be deployed on the devices to withdraw participation in a VRF.

This section contains:

- Sample Summary for Delete VRF
- Understanding VRF Configurations for Delete VRF

Note Upon successful completion of Delete VRF workflow, LMS triggers the Data Collection process. After the Data Collection process is complete, LMS initiates the VRF Collection process. The VRF Collection process initiated depends on the settings provided in Admin. See *Administration of Cisco Prime LAN Management Solution 4.1* for more information.

The Sample Summary summarizes the VRF configuration details on the devices 10.77.241.4 and 10.77.241.6. For more information, see Figure 11-3.

A sample of the summary is displayed below.

Sample Summary for Delete VRF

```
Device:10.77.241.4

   no interface Vlan5
   no ip vrf GreenVRF

Device:10.77.241.6
```

```
no interface Vlan5
no ip vrf GreenVRF
```

Understanding VRF Configurations for Delete VRF

The VRF configuration details pushed in the devices is explained in Table 11-15

Table 11-15 Delete VRF Configuration details

Command	Purpose
`Device` *device name*	Name of the device
`no interface` interface-id	Removes the interface_id from device name. For example, vlan 5 will be removed from device IP 10.77.241.6.
`no ip vrf` *vrf-name*	Deletes the VRF from the device

To delete VRF, present on the selected devices, Click **Finish** in the Summary page.

A job is created to delete the VRF configurations details from the selected devices. A confirmation message appears with the Job ID in the Information dialog box.

To view the VRF configuration job status, go to **Configuration > Job Browsers > VRF Lite**. See Using VRF Lite Job Browser.

Edge VLAN Configuration

In an Enterprise network, end-to-end virtualization is achieved by associating a VRF instance with an SVI to map VLANs to different logical or physical VPN connections.

The Edge VLAN Configuration workflow allows you to map the Access VLANs to a VRF instance there by providing end-to-end virtualization. The Access VLANs are mapped to single VRF instance by assigning it to existing Switch Virtual Interface (SVI) or new SVIs created at the Distribution Layer.

A VRF instance is associated with an Switch Virtual Interface (SVI) to map VLANs to different logical or physical VPN connections.

Note You can associate at most one SVI with a VLAN.

The following users have the privilege to assign Edge VLAN to VRF: Network Administrator and Super Admin. These user privileges apply only to the local mode.

The Edge VLAN Configuration wizard directs you through:

5. VLAN to VRF Mapping
6. Edge VLAN Configuration Summary

To perform Edge VLAN Configuration:

Step 1 Select **Configuration > Workflows > VRF-lite > Edge VLAN Configuration**.

The Edge VLAN Configuration: VRF and Device Selection page appears. Table 11-16 details the Edge VLAN Configuration: VRF and Device Selection page.

Table 11-16 Edge VLAN Configuration: VRF and Device Selection

Window Element	Description
VRF Details	
VRF Name	Shows the list of VRFs as a drop-down list. Select the VRF from the drop-down list.
Route Distinguisher (RD)	*Display only.* Shows the RD value of the selected VRF in the format *X:Y.* For more information on RD, see Route Distinguisher (RD).
Description	*Display only.* Description of the selected VRF. You cannot edit the description.
Device Selector	
Device Selector	Device Selector displays VRF-configured devices with selected VRF. The Device Selector displays the devices under the following groups: • All Devices - Represents VRF Configured devices • Device Type Groups - Represents the devices that are grouped as Routers, Switches and Hubs, and Unknown Device Type • User-defined Groups - Represents the devices that are in the user-defined groups. The Device Selector enables you to search and select the devices. Select the checkbox to select the device in the groups listed. For more information on the devices listed, see Device Selector.

Step 2 Click **Next**

The Edge VLAN Configuration: VLAN to VRF Mapping page appears.

For information on VLAN to VRF Mapping, see VLAN to VRF Mapping.

VLAN to VRF Mapping

The Edge VLAN Configuration: VLAN to VRF Mapping page is used to map the Access VLANs to a VRF instance thereby providing an end-to-end virtualization. You can assign Edge VLAN to a VRF by associating it to a Switch Virtual Interface (SVI).

The Edge VLAN Configuration: VLAN to VRF Mapping page is used to:

1. Configure SVI for new or already existing VLANs in the Distribution Layer
2. Allow VLANs in available trunk in Access Layer
3. Configure Layer 3 features

The devices selected in Edge VLAN Configuration: Select Devices page are the devices from the Distribution Layer.

The Edge VLAN Configuration: VLAN to VRF Mapping page displays a list of Switch Virtual Interfaces (SVIs) that are

- Virtualized with the VRF selected
- Unfertilized

This section contains:

- Trunk Configuration
- Layer 3 Features

The Edge VLAN Configuration: VLAN to VRF Mapping page includes the following icons:

- Existing VLAN icon: Used to display existing VLANs (VLAN Name) on the device.
- Configurations icon: Used to perform Trunk and Layer 3 feature configuration.

  Upon clicking the Configurations icon, the Trunk Configuration tab is selected by default and the Available Trunks page appears.

Step 1 The Edge VLAN Configuration: VLAN to VRF Mapping window appears. The window displays the name of the selected VRF in the Edge VLAN Configuration: Select Devices page. In this window, enter the details as given in Table 11-17.

Table 11-17 Details of VLAN to VRF Mapping

Window Element	Description	Usage Notes
VRF Details		
VRF Name : Selected VRF	Name of the VRF selected.	Display only.
Device Details		
Device Name (Hyperlink)	Represents the device selected in the Device Selector. Device name of the device is displayed as a hyperlink.	Click the arrow icon to view or hide details of the SVIs that are a part of the device name. If you right-click the Device name hyperlink, it displays Add SVI option. Click Add SVI option to add an SVI

Table 11-17 Details of VLAN to VRF Mapping

Window Element	Description	Usage Notes
Name	Represents a Switch Virtual Interface that is the logical Layer 3 interface on a switch. It displays the multiple VLANs that are carried by the physical interface. The corresponding VLAN ID and VLAN Name is populated in this page. You can view the status of the interface. It displays a tick mark if the status is up and cross mark if the status is down.	• Enter the SVI value. Valid values of SVI ranges from 2 to 4096. Or • Select existing VLANs on your network by clicking the icon. If the existing VLAN Name is displayed in this field, you can edit this field. Edited entries will overwrite the existing VLAN Name. If the VLAN value entered is not in your network, LMS creates VLAN.
Checkbox	Allows you to virtualize or un-virtualize SVIs using the selected VRF.	• To virtualize an interface, check against the SVIs listed under the Device Name • To un-virtualize, un-check an interface that is already virtualized with a VRF
Existing VLAN icon	When you click this icon, the Existing VLAN Selector page appears. This page displays the existing VLANs on the device. You can also search existing VLANs by entering the VLAN Name in the Search field. The VLANs displayed do not have an SVI/SI in the selected device.	Select the desired VLAN. Upon selecting the VLAN, the corresponding VLAN Name and VLAN ID is populated in the VLAN ID and VLAN Name field.
IP Address	IP Address of the SVI.	Enter the IP Address. Valid IP values are the IPv4 Addresses
Subnet Mask	Subnet mask of the SVI.	Enter the Subnet mask
VLAN ID	VLAN ID to be assigned to a VRF. Valid values of VLAN ID ranges from 1 to 4094.	Enter the VLAN ID. You cannot edit this field.
VLAN Name	VLAN Name to be assigned to a VRF.	Enter the VLAN Name.
Configurations	Enables you to perform the following configurations to be associated to the corresponding SVI: Trunk and Layer 3 feature configuration.	Click the Edge Interface Configuration icon to configure Trunk and Layer 3 features. For more information, see Trunk Configuration and Layer 3 Features.

Trunk Configuration

The Available Trunks page displays the trunks available in the selected device. It also displays the device that are neighbors to the selected device. If no trunk is available in the selected device, the Available Trunks page is blank.

The VLANs in any corresponding, existing or newly created SVIs will be allowed on all the trunk interfaces, that are selected in the Trunk Configuration page. The values displayed in the Trunk Configuration page are not fetched from the selected devices.

Step 2 In the Trunk Configuration page, enter the details as given in Table 11-18.

Table 11-18 Settings of Trunk Configuration

Window Element	Description	Usage Notes
Available Trunks		
Interface Name	Interface name on which Trunk exist.	Display only.
Neighbor Name	Neighbor device to the selected device.	Select the desired trunk in which VLAN needs to be allowed and click **Apply**. The Trunk configuration details entered are saved. The VLANs in the corresponding SVI will be allowed on all the trunk interfaces that are selected in the Trunk Configuration page.

Layer 3 Features

Upon clicking the Layer 3 Features tab, the Layer 3 Feature page appears which enables you to configure the following Protocols and DHCP Server details for any corresponding, existing or newly created SVIs. The values displayed under Layer 3 Features tab are not fetched from the selected devices.

- HSRP : Hot Standby Router Protocol
- VRRP : Virtual Router Redundancy Protocol
- GLBP: Gateway Load Balancing Protocol

Note The layer 3 features details are not fetched from the devices.

Step 3 In the Layer 3 Feature Configuration page, enter the details as given in Table 11-18

Table 11-19 Settings of Layer 3 Feature Configuration

Window Element	Description	Usage Notes
Layer 3 Redundancy Protocol		
Select Type	Represents the Redundancy protocol types. HSRP : Hot Standby Router Protocol VRRP : Virtual Router Redundancy Protocol GLBP: Gateway Load Balancing Protocol	Select the desired Redundancy protocol Type.

Table 11-19 Settings of Layer 3 Feature Configuration (continued)

Window Element	Description	Usage Notes
Group Number	Represents the group number of the protocol. A valid group number is an integer. Valid range values for corresponding Redundancy Protocols is as follows: • HSRP : 0 - 4095 • VRRP : 1 - 255 • GLBP : 0 - 1023	Enter the Standby Group Number.
Virtual Router IP Address	IP Address of the Virtual Router at the edge.	Enter the Virtual Router IP Address. Valid IP values are the IPv4 Addresses.
DHCP Server IP Address	IP Address of the DHCP Server	Enter the DHCP Server IP Address and click **Apply**. Valid IP values are the IPv4 Addresses. After applying the Layer 3 Features configuration details, the values are saved. Click **Close.** The Edge VLAN Configuration: VLAN to VRF Mapping page appears.

After entering the Trunk and Layer 3 Features, a new row is added on the Edge VLAN Configuration: VLAN to VRF Mapping page appears. You can enter the details in the new row to create an SVI for newly created VLAN.

Step 4 Click **Next**

The Edge VLAN Configuration: Summary page appears.

For information on Summary, see Edge VLAN Configuration Summary.

Edge VLAN Configuration Summary

The Edge VLAN Configuration: Summary page summarizes the VRF configuration details to be deployed to the selected devices.

This section contains:

- Sample Summary for Edge VLAN Configuration
- Understanding Edge VLAN Configuration Details

Note Upon successful completion of Edge VLAN Configuration workflow, LMS triggers the Data Collection process. After the Data Collection process is complete, LMS initiates the VRF Collection process.

The Sample Summary summarizes the VRF configuration details on the device 10.77.241.2. For more information, see Figure 11-2.

A sample of the summary is displayed below.

Sample Summary for Edge VLAN Configuration

```
Device:10.77.241.4

    vlan 3
        name VLAN0003
    interface VLAN3
        ip vrf forwarding GreenVRF
        ip address 10.77.22.3 255.255.255.2
        no shutdown
        glbp 1 ip 10.77.22.23
        ip helper-address 255.255.255.0
```

Understanding Edge VLAN Configuration Details

The following VRF configuration details are pushed in the selected devices. The description of the Edge VLAN Configuration details is given in Table 11-20.

Table 11-20 Edge VLAN Configuration details

Command	Purpose
ip vrf forwarding *vrf-name*	Enters VRF configuration mode and assigns a VRF name
description *vrf-name*	Provides description of the VRF created
ip address *vrf-name*	Associates a VRF with an interface or sub-interface
no shutdown	Converts Layer 2 switch port interface to a Layer 3 routed physical interface
glbp	Enables IEEE 802.1Q encapsulation of traffic on a specified sub- interface in virtual LANs. IEEE 802.1 Q is a standard protocol for interconnecting multiple switches and routers, and for defining VLAN topologies.
ip helper-address	Used to enable an interface

To assign VLANs on the selected interfaces, to a VRF, click **Finish** in the Edge VLAN Configuration: Summary page.

A job is created to assign edge VLAN to the selected VRF. A confirmation message appears with the Job ID in the Information dialog box.

To view the VRF configuration job status, go to **Configuration > Job Browsers > VRF Lite**. See Using VRF Lite Job Browser.

Using VRF Lite Job Browser

The VRF Lite Configuration Jobs browser enables you to view the status of all VRF configuration Jobs. VRF configuration jobs are the jobs that are created for the VRF configuration workflows like Create, edit, extend and delete VRF as well as Edge VLAN Configuration jobs.

The job details that you can view here, include the job ID, the job type, the job description, the job owner, the time the job is scheduled to run at, the time of job completion, the schedule type, the job status, run status. Table 11-21 describes the fields in the VRF Lite Configuration Jobs browser.

To access the VRF Lite Configuration Jobs browser, select **Configuration > Job Browsers > VRF Lite**. The VRF Lite Configuration Jobs browser page appears.

You can manage the VRF configuration jobs using the VRF Lite Configuration Jobs browser.

Note View the Permission Report (Reports > System > Users > Permission) to check whether you have the required privileges to perform this task.

The VRF Lite Configuration Jobs browser is used to perform the following:

- View—Used to launch reports. See View.
- Stop—Stop a scheduled or running job. See Stop Job.
- Retry—Retry a job. See Retry Job.
- Delete—Delete a job. See Delete Job.

Table 11-21 VRF Lite Configuration Jobs Browser

Field	Description
Job ID	Unique ID assigned to the VRF configuration job when it is created. Clicking the Job ID hyperlink provides a report page with the job details of the job.
Job Type	Type of VRF configuration job such as Create VRF, Edit VRF, Extend VRF, Delete VRF and Edge VLAN Configuration.
Description	Description of the job provided by the job creator.
Owner	User who created the job.
Scheduled At	Date and time the job was scheduled at.
Completed At	Date and time the job was completed at.

Table 11-21 VRF Lite Configuration Jobs Browser

Field	Description
Run Status	Job states include: • Running • Waiting for approval • Scheduled (pending) • Succeeded • Succeeded with Info • Failed • Crashed • Cancelled • Suspended • Rejected • Missed Start • Failed at Start
Schedule Type	Specifies the type of schedule for the job: • Once—Runs once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. • Immediate—Runs immediately.
Status	Provides the status of the current jobs. The status of the current jobs is displayed as succeded or failed.

View

Use to launch the respective report of the VRF configuration job selected in the VRF Lite Configuration Jobs Browser page.

Stop Job

You can stop a scheduled or running job from the VRF Lite Configuration Jobs Browser.

Select the job and click **Stop**. You are prompted for a confirmation before the job is stopped. You can select only one job to stop at a given time.

Delete Job

You can delete a VRF configuration job from the VRF Lite Configuration Jobs Browser.

Select the job and click **Delete**. You are prompted for a confirmation before the job is deleted. You can select more than one job to delete.

Retry Job

You can retry a VRF configuration job related to VRF configuration from the VRF Lite Configuration Jobs Browser. You can retrieve only failed jobs.Select the job and click **Retry**. You are prompted for a confirmation before retrying the job. You can select only one job to be retried at a given time.

CHAPTER 12

Viewing Topology Services

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

Topology Services displays the network topology of the devices discovered by LMS through Topology Maps. Besides these Maps, the application includes numerous reports that helps you to view the physical and logical connectivity in details.

To launch Topology Services, either:

- Select **Configuration > Topology** from the menu.

Or

- Select **Monitor > Monitoring Tools > Topology Services** from the menu.

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.

See *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1* for more information.

APPENDIX 13

CLI Utilities

LMS provides Command Line Interface (CLI) support. The CLI utilities that are supported by LMS are:

- CWCLI
- Performance Tuning Tool
- syslogConf.pl Utility
- Software Management CLI Utility

CWCLI

CiscoWorks Command Line Framework (CWCLI) is the interface or framework through which application functionality is provided.

The following are the `cwcli` applications:

- `cwcli config` is the configuration command-line tool. `cwcli netconfig` command lets you use NetConfig from the command line.
- `cwcli export` is a command line tool that also provides servlet access to inventory, configuration and change audit data.

  This can be used for generating inventory, configuration archive, and change audit data for devices in LMS.
- `cwcli inventory` is a Device Management application command line tool. This tool can be used for checking the device credentials, exporting the device credentials. You can also view the devices and delete the devices.
- `cwcli invreport` is a CiscoWorks command line tool which allows you to run previously created Inventory Custom Reports and also system reports. The output is displayed in the (CSV) Comma Separated Value format.
- `cwcli netshow` is a comand line tool that lets you use NetShow features from the command line. You can use the cwcli netshow commands to view, browse, create, delete, and cancel NetShow jobs and Command Sets.

This chapter contains the following sections:

- Overview: CLI Framework (cwcli)
- Overview: cwcli config Command
- Overview: cwcli netconfig Command
- Overview: cwcli export Command

- Overview: cwcli inventory Command
- Overview: cwcli invreport Command
- Overview: cwcli netshow Command

You can set the debug mode for CLIFramework and ConfigCLI in the Log Level Settings dialog box (**Admin > System Preferences > Loglevel Settings**).

Overview: CLI Framework (cwcli)

CLI Framework (`cwcli`) is a Command-Line Interface (CLI). This interface provides application-related functionality.

The CLI Framework supports the following tasks:

- Parsing the command line for the applications.
- Easy logging and messaging capabilities
- Authentication and authorization for individual applications
- Remote access support.

This section contains:

- cwcli Global Arguments
- Remote Access

SYNOPSIS

The command line syntax is as follows:

`cwcli` *application command GlobalArgs AppSpecificArguments*

- *application* specifies one or more LMS applications that use the framework. For example, config, export, inventory, invreport, and netconfig.
- *command* specifies which core operations are to be performed for a particular service.
- *GlobalArgs* specifies arguments common for all CLI. For example, username, password, log, debug, etc.
- *AppSpecificArguments* are the additional parameters required for each core command.

You should enter the application name immediately after `cwcli` and the command name, after the application name. All other GlobalArgs arguments can be specified in any order.

Apart from the applications, Global args (`-u` *user*, `-p` *password*, `-l` *logfile*, `-m` *email*, `-d` *debuglevel*) framework also supports two generic commands. They are:

- `-v`—Version of the CLI interface.
- `-help`—All the applications that can be invoked using the framework.

SYNTAX

```
cwcli  -v
cwcli  -help
```

cwcli Global Arguments

The following table shows the **cwcli config** command arguments you can specify with all commands.

cwcli arguments	Description
-u *userid*	User ID. Field is required.

-p *password*	It is the password for the specified User ID.
	If you enter the password at the command line, a message appears:
	`* Warning * The -p option is highly insecure and *not* recommended. See -u option for more details.`
	If the password is not specified in the command line, framework searches for the password in the file pointed to by the CWCLIFILE environment variable. If the variable is not set, you are prompted to enter the password.
	`* Warning * CWCLIFILE Environment variable not set. Enter your password`
	See Setting CWCLIFILE Environment Variable for more details.

-device *devicename* or *device_list*	Display name of the device added into DCR. You can use comma separated displaynames and wild card character **%**. For example, if there are two devices with names Rtr12 and Rtr13, Rtr% will display both the devices. To use all the devices, use **-device** %.
-view *view_list*	If the data needs to be generated for all the devices in a specific group, you can use the **-view** argument. You can use this argument to generate data for devices in all device views including system-defined groups and user-defined groups. You can enter multiple group name separated using a comma. For view name, you have to enter the fully qualified path as in the Group Administration window. To separate the path you must use forward slash only. For example, **-view** "/RME@*ciscoworks_servername*/All Devices"
-ipaddress *address*	Device IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated. You cannot use this option with **-device**, **-view** , or **-input**. Also, you cannot specify wildcard characters.
-l *logfile*	Must be a relative name. By default ConfigCLI.log and cli.log files are used, located at: • *NMSROOT*\log (On Windows) • /var/adm/CSCOpx/log (On Solaris and Soft Appliance) If the relative name is specified then the log messages are logged into the file specified. The file is created under the log directory, mentioned above. For example, **cwcli config export -u** *alpha* **-p** *beta* **-device % -l** *export.log.* In this case, export.log is created under the log directory mentioned above.
-m *email*	Email address to mail the command output to. You can enter single or comma separated email IDs.
-d *debuglevel*	Enables debugging to command-line tool. Specifies debugging verbosity. Default is least verbose.

cwcli arguments	Description
`-help`	Displays usage information.
`-input`	Text file containing arguments for each device.

Note `-d` and `-l` arguments are supported for backward compatibility. Select **Admin > System > Debug Settings > Config and Image Management Debugging settings > CLI Framework** to set debug levels.

When using wildcards, you must use the percent sign (`%`), not an asterisk (`*`), as shown in the following examples:

```
%device (lists all devices that end with the suffix 'device')
dev% (lists all devices that start with the prefix 'dev')
% (lists all devices LMS manages)
```

Remote Access

CLI framework (**`cwcli`**) offers remote access facilities to allow you to invoke **`cwcli`** commands from the client in the same way as they run on the LMS server.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to run any command:

For post request,

`http://`*lms-server:lms-port*`/rme/cwcli`* *payload XML file*

For get request,

`http://`*lms-server:lms-port*`/rme/cwcli?command=cwcli config`* *commandname* `-u` *user* `-p` *BAse64 encoded pwd -args1 arg1value...*

Note Use <arg> and <argval> tags when the argument is a file.

The contents of the payload xml file is as follows.

```
<payload>
   <command>
    cwcli config export -u admin -p <Base64Enoced pwd> -device 1.1.1.1 -xml
   </command>
   <arg>
   </arg>
   <arg-val>
   </arg-val>
</payload>
```

For example to run the **`cwcli config import`** comand payload.xml is as follows:

```
<payload>
   <command>
     cwcli config import -u admin -p <Base64Enoced pwd> -device 10.77.240.106
     <arg>
```

```
      -f
      </arg>
      <arg-val>
       tempfile
      </arg-val>
    </command>
</payload>
```

The Remote Access servlet creates a temporary file with the contents specified between the arg-val tags for the **import** command. On the server the command is run as
cwcli config import -u *admin* **-p** *Base64Enoced pwd* **-device** *10.77.240.106* **-f** *tempfile*

Here, the tempfile contains the configuration of the device that you want to import.

For example,

perl samplescript.pl http(s)://*lms-server:lms-port***/rme/cwcli** *payloadXML*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

Note For the secure mode (HTTPS) the port number is 443. The default port for LMS server in HTTP mode is 1741.

Sample Script to Invoke the Servlet

```
#!/opt/CSCOpx/bin/perl
use LWP::UserAgent;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
print "\n argv[0} = $ARGV[0] , fname = $fname \n";
open (FILE,"$fname") || die "File open Failed $!";
while ( <FILE> )
{
$str .= $_ ;
}
#print $str ;
url_call($temp);
#-- Activate a CGI:
sub url_call
{
my ($url) = @_;
my $ua = new LWP::UserAgent;
$ua->timeout(1000);
# you can set timeout value depending on number of devices
my $hdr = new HTTP::Headers 'Content-Type' => 'text/html';
my $req = new HTTP::Request ('GET', $url, $hdr);
$req->content($str);
print "It comes here \n";
my $res = $ua->request ($req);
```

```
my $result;
#    print "It comes here too \n";
if ($res->is_error)
{
print "ERROR : ", $res->code, " : ", $res->message, "\n";
$result = '';
}
else {
    $result = $res->content;
       if($result =~ /Authorization error/)
{           print "Authorization error\n";
          }
else {
print "\n $result" ;
         }
     }
}
```

Setting CWCLIFILE Environment Variable

You can store your username and password in a file and set a variable *CWCLIFILE* which points to the file, if you want to avoid the **-p** argument which will reveal the password in clear text in CLI.

You should maintain this file and control access permissions to prevent unauthorized access.

If *CWCLIFILE* is set only to filename instead of full path, **cwcli** framework looks for the current working directory.

If you use the **-p** argument, even after setting the *CWCLIFILE* variable, the password is taken from the command line instead of *CWCLIFILE*. This is not secure and usage of this argument is not recommended.

The password must be provided in the file in the following format:

username password

Where username and password are the LMS login credentials. The delimiter between the username and password is a single space.

You must enter a comma as the delimiter if the password is blank. Otherwise, `cwcli` framework will fail to validate the password.

Example to run the cwcli command with the `CWCLIFILE` file:

On Windows, at the command prompt enter:

`C:\Program Files\CSCOpx\bin>`**`set CWCLIFILE=`***`D:\ciscoworks\password.txt`*

`C:\Program Files\CSCOpx\bin>`**`cwcli export changeaudit -u`** *admin* **`-view`** "/**`RME@`***ciscoworksservername*/*Normal Devices*"

Where the file, password.txt contains the username and password for LMS server.

Overview: cwcli config Command

The **`cwcli config`** command-line tool performs the following core functions on one or more devices and the configuration archive:

- Moves configuration files from the configuration archive to one or more devices.
- Transfers the configuration files from devices to the archive if the configuration running on a device is different from the latest archived version
- Imports configuration files from the file system and pushes them to one or more devices, which updates the configuration archive
- Merges the startup configuration files with the running configuration files
- Copies the running configuration files to the startup configuration files
- Copies a configuration file to the startup configuration files
- Copies the difference between a configuration file and the running configuration to the running configuration files. This makes the configuration in the file available on the running configuration.
- Reboots running devices to load a running configuration with its startup configuration

In addition, **`cwcli config`** performs the following core functions on the configuration archive:

- Exports configurations from the archive to the filesystem
- Compares any two configuration files in the archive based on version or date
- Deletes configurations older than a specified date from the configuration archive

This section contains:

Using the cwcli config Command for Batch Processing

In addition to using the graphical-based device configuration functions, you can use the **`cwcli config`** command-line utility to perform batch processing tasks on the configuration archive, devices, or on both.

For more details see these sections:

On platforms other than Windows 2000, all files created by **cwcli config** are owned by casuser. They belong to the same group as the user (casuser) who created the files, and have read-write access for both casuser and the group.

Note Your login determines whether you can use this argument.

Getting Started With cwcli config

cwcli config is a command-line tool. This tool is like an interface between the user and the device and the configuration archive.

Generally, the configuration archive automatically registers modifications to the device's configuration in archived, version-based files. Over time, multiple configurations of a device accumulate in the archive. Typically, the latest version is the configuration running on the device.

Uses of cwcli config

With **cwcli config**, you can:

- Device and Archive Updates

  Modify a device's running configuration. You can allow personnel of your organization to modify the device's configuration without explicitly providing them with Telnet access to the device.

- Deleting Configurations

  Delete unwanted versions of the configuration file from the archive. This is a command-line variant of the UI purge feature.

- Comparing Configurations

  Generate 'diffs' of different configuration versions of the same device to find out what modifications were made. This is a command-line counterpart for GUI-based reports.

Device and Archive Updates

Whenever you use **cwcli config** to update the running configuration of the device, the tool also archives the newly written configuration to the archive, bypassing the auto-detection mechanism.

Getting a Version of the Device Configuration

To obtain a version of the device's configuration from the device, modify it, and then write it back to the device. You use two features of **cwcli config** to do this.

1. Use the **export** command to obtain a copy of the desired configuration version file.
2. Edit and deploy it on the device using the **import** function. If the update succeeds, **import** also archives the configuration in the archive as the latest version.

Example:

cwcli config export -u *user* **-p** *pass* **-device** *zebra.domain.com* **-version** *3* **-f** *zebraconf*

version 3 of device zebra's configuration has been obtained from the device. It is available in the file zebraconf. You must edit the file and make the necessary modifications.

```
cwcli config import -u user -p pass -device zebra.domain.com -f zebraconf
```

The edited file is written back to the device and archive. If there were five configurations originally, a sixth one is now added.

If you want to update the running config on the device, and are certain that the latest archived version is the same as the running config, then you can obtain the latest version as follows:

cwcli config export -u *user* **-p** *pass* **-device** *zebra.domain.com* **-f** *zebraconf*

the latest version is copied to file zebraconf.

After writing the edited configuration to the device, you might want to reboot the device. You can do this automatically from **cwcli config** by using the **-reboot** argument to the **import** command:

cwcli config export -u *user* **-p** *pass* **-device** *zebra.domain.com* **-f** *zebraconf* **-reboot**

In addition, you might want to write file zebraconf to both the running as well as the startup configuration. To do this, enter the following command:

cwcli config export -u *user* **-p** *pass* **-device** *zebra.domain.com* **-f** *zebraconf* **-save**

Reverting to Earlier Configuration Version

For running configuration, use either compare or export to decide, which version to revert to.

For VLAN configuration, look into the Configuration Version Report for the device to find the versions for which VLAN configuration is also archived. Then use **put** to deploy the desired version.

The **put** function gets the requested version from the archive, writes it to the device. For Running configuration, it archives it as the latest version of that device.

Example:

cwcli config put -u *user* **-p** *pass* **-device** *zebra.domain.com* **-version** *3*

version 3 of device zebra's configuration is extracted from the archive and written to the device. It is also stored in the archive as the latest version.

Example:

cwcli config put -u *user* **-p** *pass* **-device** *zebra.domain.com* **-version** *3* **-filetype** *vlan*

version 3 of device zebra's vlan configuration is extracted from the archive and written to the device.

Like **import**, the **put** function allows you to reboot the device using the **-reboot** argument, and to update the startup configuration using the **-save** argument.

Writing Startup Configuration to Running Configuration

To write the startup configuration of the device to its running configuration. Use the **start2run** function of **cwcli config** to retrieve the startup configuration from the device, and then write it back to the device's running configuration. The new running configuration is archived as the latest version.

Example:

cwcli config start2run -u *user* **-p** *pass* **-device** *zebra.domain.com*

To ensure that the running configuration on the device is stored in the archive, that is, synchronize the archive with the device. Use the get function to do so.

Example:

cwcli config get -u *admin* **-p** *admin* **-device** *zebra.domain.com*

The running configuration of device zebra is retrieved from the device and archived as the latest version, only if there is a need to do so. However, if the running configuration does not differ from the latest archived version, then the archival does not take place.

Configuration updates can be performed on multiple devices at once. For more details see "Running cwcli config on Multiple Devices" section on page 13-11.

Deleting Configurations

Use the `delete` function of `cwcli config` to delete unwanted versions from the archive, to conserve disk space, and to reduce visual clutter on reports.

Example:

`cwcli config delete -u` *user* `-p` *pass* `-device` *zebra.domain.com* `-version` *2 5*

All versions between and including 2 and 5 are removed from the archive. There is also a time-stamp based variant.

Comparing Configurations

Use the `compare` function to compare any two versions of the archived configuration files of one or more devices. The compare function also lists down the entire configuration changes based on the timestamp.

Example:

`cwcli config compare -u` *user* `-p` *pass* `-device` *zebra.domain.com* `-version` 2 5

`cwcli config` can only compare the archived configuration files. The compliance report is stored in the job directories.

Remote Access

`cwcli config` uses remote access facilities offered by the CLI framework to allow you to invoke the `cwcli config` commands from the client in the same manner they would run them on the LMS server.

The name of the servlet is /rme/cwcli.

All the command can be run remotely.

Note For the secure mode (HTTPS) the port number is 443. The default port for LMS server in HTTP mode is 1741.

Running cwcli config

The `cwcli config` command is located in the following directories, where install_dir is the directory in which LMS is installed:

- On Solaris and Soft Appliance systems, *NMSROOT*/bin. The default directory is /opt/CSCOpx
- On Windows systems, *NMSROOT*\bin

  The default install directory is C:\Program Files.

If you install LMS on Windows on an NTFS partition, only users in the administrator or casuser group can access `cwcli config`.

Users with read-write access to the CSCOpx\files\archive directory and the directories under that can also use `cwcli config`.

Running cwcli config on Multiple Devices

You can run **cwcli config** simultaneously on multiple devices. Details vary from command to command. This section describes how to apply import on multiple devices. Details of multiple-device syntax for other commands are described under the DESCRIPTION in the man page.

The commands, such as **put**, **import**, **write2run** and **write2start** accept only one device on the command line. If you want to apply the command to multiple devices, enter the names of those devices and any arguments in a text file.

For example, assume that you want to deliver the configuration file serviceconf to devices, antelope and rhino. Also assume that you want to reboot rhino. The command line of **cwcli config** is as follows:

cwcli config import -u *admin* **-p** *admin* **-input** *device-list* **-m** *root@netcontrol.domain.com*

You do not want the output of the command to go to stdout. Instead, you want it to be mailed to the superuser at host netcontrol.

Device-list is a text with the following contents:

```
# comments start with a leading hash symbol. Write serviceconf to rhino and # antelope.
reboot antelope.
-device rhino.domain.com -f serviceconf
-device antelope.domain.com -f serviceconf -reboot
# end of input file device-list
```

Additional Information

The examples in this man page are not comprehensive. There are many other scenarios in which **cwcli config** can be used.

For example, if you want to modify the running configuration on the device, without using the latest archived version, considering the latest may not be the same as the running configuration. You can apply the get command and then export and import. Various combinations of the features can be used.

You can also use **cwcli config** in UNIX cron jobs to schedule config updates in advance.

Also, the output generated by **cwcli config** can be logged to a file and sent to any recipient through email. A host of additional arguments can be applied on other commands.

cwcli config Command Parameters

Using the **cwcli config** commands you can manipulate, deploy and archive your device configuration files.

Using the Compare Command

When you specify the **compare** command, both **-version** and **-date** are optional.

- If you do not specify **-version** or **-date**, the latest configuration is compared with the previous version.

- If you do specify `-version` or `-date`, and the value you enter is the latest version or date, that configuration is compared with the previous version.

Using the Delete Command

When you specify the `-date` command, you must specify `-version` or `-date`.

If you specify only one date, all versions archived up and including that date are deleted.

To delete a version archived on a particular date, specify two dates that are the same date as the archived version date. The latest two versions of configuration can never be deleted from the archive. Be careful while using the `delete` command.

Parameters For All cwcli config Commands

The `-d` and `-l` arguments are supported for backward compatibility.

In LMS, select **Admin > System > Debug Settings > Config and Image Management Debugging settings > ConfigCLI** to set debug levels.

When using wildcards, you must use the percent sign (%), not an asterisk (*), as shown in the following examples:

```
%device
dev%
%device%
```

The following table lists the `cwcli config` command-specific arguments and which commands you can use the arguments with:

cwcli config arguments	Applicable Commands	Description
`-baseline`	`createdeployparamfile`, `directbaselinedeploy`	Specifies the name of the Baseline template for which the parameter file has to be created.
`-date`	`compare`, `delete`	• Compare – If you specify one date, the latest configuration version is compared with the most recently archived version on that particular date. – If you specify two dates, the most recently archived version of the first date is compared with the most recently archived version of the second date. • Delete – If you specify one date, all versions archived up to this date are deleted. – If you specify two dates, all versions archived between and on those dates are deleted.
`-enable_pass`	`import`, `put`, `write2run`, `write2start`, `run2start`, `start2run`, `deploycomplianceresults`, `compareanddeploy`, `reload`	Specifies execution mode Base64 encoded Password for connecting to device.

cwcli config arguments	Applicable Commands	Description
-f *filename*	**export**, **import**	Specifies fully qualified pathname of configuration file to import to or export from. • If you do not specify this argument, the current working directory is assumed. • If you do not specify this argument when importing or exporting a single device configuration, default filename, devicename.cfg, in the current working directory is assumed. The **-f** argument applies only to single devices. To perform the operation on multiple devices, you must specify the **-input** argument.

-input *inputlist*	Applicable to all commands except **compareanddeploy**, **createdeployparamfile**, **deploycomplianceresults**, and **directbaselinedeploy**,	You must enter **-input** inputlist to run commands, such as put and import, on multiple devices.
		The parameter, inputlist is a text file containing arguments for each device. A line starting with # is treated as a comment.
		For example, an input list file might look like this:
		`#comment line`
		`-version version [-save] [-reboot] device_name`
		`-version version [-save] [-reboot] device_name`

-jobid	**createdeployparamfile**	Used to specify the job identifier of the previously run comparewithbaseline job.
-l	**createdeployparamfile**, **directbaselinedeploy**	Specifies the file to log the results of the command.
-listonly	**write2run**	Displays difference between the latest running configuration for device in configuration archive and new configuration that is generated, without downloading changes.
-m	**createdeployparamfile**, **directbaselinedeploy**	Specifies an email address to send the results of the command.
primary_pass	**import**, **put**, **write2run**, **write2start**, **run2start**, **start2run**, **deploycomplianceresults**, **compareanddeploy**, **reload**	Specifies primary user name for connecting to device.
-primary_user	**import**, **put**, **write2run**, **write2start**, **run2start**, **start2run**, **deploycomplianceresults**, **compareanddeploy**, **reload**	Specifies primary user name for connecting to device.
-reboot	**import**, **put**	After successfully pushing a configuration to a device, device reboots. By default the device does not reboot. For IOS devices, you must also specify -save to avoid losing configuration changes when rebooting.
-save	**import**, **put**	Applies to Cisco IOS devices only. Performs a write memory after pushing the configuration. The default is no write memory.

cwcli config arguments	Applicable Commands	Description
`-timeout`	**import**, **put**, **write2run**, **write2start**, **run2start**, **start2run**, **comparewithbaseline**, **deploycomplianceresults**, **compareanddeploy**, **get**, **reload**	Specifies the duration of the interval in seconds between two successive polling cycles. Configuration Archive is polled according to the interval specified to retrieve and display the job results.
`-version` *version*	**compare**, **delete**, **export**, **put**	• For put and **export**, you can specify one version of the configuration in the archive. • For compare, you can specify two versions, which are compared with each other. If you specify only one version, that is compared with latest archived version. • For delete, if you specify one version, that version is deleted. If you specify two versions, all versions in between and including those version are deleted.

cwcli config Syntax Examples

The following examples demonstrate the **cwcli config** command syntax. Square brackets ([ ]) indicate arguments. A pipe (|) acts as a delimiter. This means that only one of the listed entries can be specified.

Note Make sure you first use the **cwcli config** command in a test environment before running the command in production. This is to avoid any loss of data when a device is rebooted or a configuration is overwritten.

The following command extracts the running configurations from all devices:

```
cwcli config get -u user -p password -device %
```

The following command exports the configuration of all the devices from the archive and puts the configuration into the file, devicename.cfg. This is the default file name because **-f** is not specified:

```
cwcli config export -u user -p password -device %
```

If there is more than one device in the default view All, you see an error message because the **export** command does not accept multiple device names on the command line. You must specify the **-input** argument to run the **export** command on more than one device.

The following table shows more syntax examples:

Argument	Syntax	Notes
no arguments	**cwcli config -u** *user* **-p** *password* [**-v -help**]	If you do not specify arguments, **cwcli config** shows command usage (**-help**)
compare	**cwcli config compare -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* } { **-version** *version1* [*version2*] | **-date** *date1* [*date2*] }	Specify versions to compare using **-version** or **-date** argument. When specifying a date, use format mm/dd/yyyy. If you do not specify a date or a version, the latest two archived configurations are compared.
compareanddeploy	**cwcli config compareanddeploy -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] {**-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* }{ **-baseline** *baselinefile* }[**-timeout** *seconds*] [**-input** *argumentFile*] [**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*]	Creates a job that compares the given Baseline template with the latest version of the configuration for a device and downloads the configuration to the device if there is non-compliance.
comparewithbaseline	**cwcli config comparewithbaseline -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* }{ **-baseline** *baselinefile* }[**-timeout** *seconds*] [**-input** *argumentFile*]	Creates a job that compares the given Baseline template with the latest version of the configuration for a device. In case of non-compliance, the non-compliant commands are displayed.
delete	**cwcli config delete -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* } { **-version** *version1* [*version2*] | **-date** *date1* [*date2*] }	Deletes the specified device configuration from the archive. Use **-date** or **-version** argument to specify configurations to delete. If you specify two dates, all configurations archived between those dates are deleted. If you specify two versions, all configurations between and including the versions are deleted.
deploycomplianceresults	**cwcli config deploycomplianceresults -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-substitute** *datafile* } {**-jobid** *jobID*}[**-timeout** *seconds*][**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*]	Creates a job that uses the previously executed **comparewithbaseline** job to get the non-compliance commands and create a job. It replaces the parameters in the non-compliant commands with the values from the data file. The commands are then downloaded to ensure compliance with the baseline configuration.
export	**cwcli config export -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *displayName* **-view** *name* | **-ipaddress** *list* } [**-f** *filename*] **[-version** *number*] [**-xml**] [**-input** *argumentFile*]	Retrieves a configuration version for a device from the archive and writes it to a file. Exported configurations are named devicename.cfg if **-f** argument is not used.

Argument	Syntax	Notes
`get`	`cwcli config get -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*] [`-l` *logfile*][`-timeout` *seconds*] [`-filetype` *running|startup|runningstartup*] { `-device` *list* | `-view` *name* | `-device` *list* `-view` *name* |`-ipaddress` *list* }	Creates a job that fetches the configuration from the device and stores it in the archive.
`import`	`cwcli config import -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*] [`-l` *logfile*][`-timeout` *seconds*] { `-device` *displayName* |`-ipaddress` *address* } [`-f` *filename*] [`-save` [`-reboot`]][`-input` *argumentFile*]	Creates a job that retrieves the configuration from a file and transfers it to the device. The job is added to the device running configuration. It then polls Configuration Archive at periodic intervals to get the job results and display it. Specify `-input` to operate on more than one device. You cannot specify wildcards or more than one device.
`listversions`	`cwcli config listversions -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*] [`-l` *logfile*] { `-device` *list* | `-view` *name* | `-device` *displayName* `-viewname` | `-ipaddress` *list*} `-baseline`	Lists the versions of the configuration archived for a device on the main branch or the Baseline templates applicable to a device.
`put`	`cwcli config put -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*] [`-l` *logfile*] { `-device` *displayName* |`-ipaddress` address `-version` *number*}[`-config` *1|2*][`-save` [`-reboot`]] [`-input` *argumentFile*][`-timeout` *seconds*] [`-filetype` *vlan|running*][`-primary_user` *primary user name*] [`-primary_pass` *Base64 encoded primary password*] [`-enable_pass` *Base64 encoded enable password*]]	Creates a job that retrieves the configuration from the configuration archive and pushes it to the device. Specify `-input` to operate against more than one device. You cannot specify wildcards or more than one device. You must specify a version.
`reload`	`cwcli config reload -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*][`-l` *logfile*] { `-device` *list* | `-view` *name* | `-device` *list* `-view` *name* |`-ipaddress` *list* }[`-input` *argumentFile*][`-timeout` *seconds*][`-primary_user` *primary user name*] [`-primary_pass` *Base64 encoded primary password*] [`-enable_pass` *Base64 encoded enable password*]	Creates a job that reboots devices. The configuration loaded runs with the startup configuration.
`run2start`	`cwcli config run2start -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*][`-l` *logfile*]{ `-device` list | `-view` *name* | `-device` *list* `-view` *name* | `-ipaddress` *list*}[`-config` 1|2] [`-input` *argumentFile*][`-timeout` *seconds*][`-primary_user` *primary user name*] [`-primary_pass` *Base64 encoded primary password*] [`-enable_pass` *Base64 encoded enable password*]	Creates a job that overwrites the startup configuration of device with running configuration. Specify multiple devices with `-device` argument by separating each device name with comma or with `-input` argument, which takes filename containing the multiple devices as an argument.

Argument	Syntax	Notes
`start2run`	`cwcli config start2run -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*][`-l` *logfile*] { `-device` *list* | `-view` *name* | `-device` *list* `-view` *name* | `-ipaddress` *list* } [`-config` 1|2] [`-input` *argumentFile*][`-timeout` *seconds*] [`-primary_user` *primary user name*] [`-primary_pass` *Base64 encoded primary password*] [`-enable_pass` *Base64 encoded enable password*]	Creates a job that merges the startup configuration with running configuration. Specify multiple devices with `-device` argument by separating each device name with comma or with `-input` argument, which takes filename containing the multiple devices as an argument.
`write2run`	`cwcli config write2run -u` *userid* `-p` *password* [`-d` *debuglevel*][`-m` *email*][`-l` *logfile*] { `-device` *displayName* | `-ipaddress` *address* } `-f` *filename* [`-config` *1|2*][`-listonly`][`-input` *argumentFile*][`-timeout` *seconds*][`-primary_user` *primary user name*][`-primary_pass` *Base64 encoded primary password*][`-enable_pass` *Base64 encoded enable password*]	Creates a job that downloads the differences between the specified file and the latest version in the archive for the specified device. If you specify `-listonly`, difference is displayed but no changes are downloaded. To run command on multiple devices, use `-input` argument, which takes a filename as an argument.
`write2start`	`cwcli config write2start -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*][`-l` *logfile*] { `-device` *displayName* | `-ipaddress` *address* `-f` *filename*} [`-config` 1|2][`-input` *argumentFile*][`-timeout` *seconds*][`-primary_user` *primary user name*][`-primary_pass` *Base64 encoded primary password*] [`-enable_pass` *Base64 encoded enable password*]	Creates a job that erases contents of device startup configuration and writes contents of given file as new startup configuration. You must specify a filename. To run a command against multiple devices, use `-input` argument.

Argument	Syntax	Notes
`collectiondate`	`cwcli config collectiondate -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*] [`-l` *logfile*] [`-filetype` *running*|*startup*|*vlan*] [`-input` *argumentFile*] { `-device` *list* `-view` *name* |`-ipaddress` *list* }	Displays the last config collection date for the devices. You can specify a filename by using the `-input` argument. The input file should be of this format: `-device` 1.1.1.1,2.2.2.2,3.3.3.3 `-filetype` *vlan* or `-filetype` *vlan* `-device` 1.1.1.1,2.2.2.2,3.3.3.3 The `-filetype` should be either vlan, running or startup. If `-filetype` is not specified, then running will be taken as the default filetype value. The output contains device name, time of last config collection, and the filetype separated by comma.
`accessdate`	`cwcli config accessdate -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*] [`-l` *logfile*] [`-filetype` *running*|*startup*|*vlan*] [`-input` *argumentFile*] { `-device` *list* `-view` *name* |`-ipaddress` *list* }	Displays the last config collection attempt date for the devices. You can specify a filename by using the `-input` argument. The input file should be of this format: `-device` 1.1.1.1,2.2.2.2,3.3.3.3 `-filetype` *vlan* or `-filetype` *vlan* `-device` 1.1.1.1,2.2.2.2,3.3.3.3 The `-filetype` should be either vlan, running or startup. If `-filetype` is not specified, then running will be taken as the default filetype value. The output contains device name, time of last attempt, and the filetype separated by comma.

cwcli config Core Arguments

cwcli config Argument	Description
`compare`	Compares last two configurations in archive, specific configuration versions, or configuration changes based on a specified date. To run this command on multiple devices, specify `-device` argument or `-input` argument.
`delete`	Deletes configurations older than specified date or version from archive. To run this command on multiple devices, specify `-device` argument or `-input` argument.
`export`	Retrieves latest configuration from archive and writes it to specified file. To run this command on multiple devices, specify `-input` argument.

cwcli config Argument	Description
`get`	Pulls configuration from device to configuration archive if configuration is different from latest archived configuration. To run this command on multiple devices, specify `-device` argument or `-input` argument.
`import`	Imports configuration from specified file and pushes it to devices. To run this command on multiple devices, specify `-input` argument.
`put`	Pushes configuration files from the configuration archive to device based on version. To run this command on multiple devices, specify `-input` argument.
`reload`	Reboots devices to reload running configuration with startup configuration. To run this command on multiple devices, specify `-device` argument or `-input` argument.
`run2start`	Overwrites startup configuration with running configuration. To run this command on multiple devices, specify `-device` argument or `-input` argument.
`start2run`	Merges startup configuration with running configuration. To run this command on multiple devices, specify `-device` argument or `-input` argument.
`write2run`	Downloads difference between latest running configuration for the device in configuration archive with configuration in file specified by -f argument. To run this command on multiple devices, specify `-input` argument.
`write2start`	Erases the contents of the device's startup configuration and writes the contents of the given file as the device's new startup configuration. To run this command on multiple devices, specify `-input` argument.
`collectiondate`	Displays the last config collection date for the devices. To run this command on multiple devices, specify `-device` argument or `-input` argument.
`accessdate`	Displays the last config collection attempt date for the devices. To run this command on multiple devices, specify `-device` argument or `-input` argument.

Examples of cwcli config

The following **`cwcli config`** command retrieves configurations for all devices in the LMS home_routers domain and stores the configurations in Sybase:

```
cwcli config get -u adam -p max -view home_routers
```

where home_routers is a device view.

The following **`cwcli config`** command reads inputfile and, for each device listed, pushes the appropriate configuration to that device:

```
cwcli config import -U adam -P max -input /tmp/inputfile
```

cwcli config Command Man Page

This man page is also accessible from the command line of a LMS server installed on a UNIX system.

To view the man page, add the path install_dir/CSCOpx/man to the MANPATH variable. Then you can enter the command man **`cwcli config`** from any directory.

You can also access man pages for each **cwcli config** command by entering the command man cwc-command, where command is the command name (for example, **export**).

The man pages for each subcommand are also available in this help system.

NAME

cwcli config LMS command line interface for the device configuration archive

SYNOPSIS

cwcli config *command* {**-arg1** [*arg1Value*] **-arg2** [*arg2Value*] **-argN** [*argNValue*]}

cwcli config -help

DESCRIPTION

cwcli config is a LMS command line tool that allows you to access the configuration archive or configurations on devices. You can use **cwcli config** to update, export, and import configurations on devices and in the archive. You can also compare configurations and delete old configurations.

To get a list of supported commands, run the command

cwcli config -help

or

cwcli config?

Help on each command can be obtained in the following manner:

cwcli config *command* **-help**

For example:

cwcli config export -help

Additionally, man pages are available on UNIX installations for individual commands. To view the man page for any command, enter:

man cwc-*command*

For example:

man cwc-export

Arguments

Many of the arguments are common across all commands. These arguments can be broadly classified as those that are expected by every command (function independent) and those that are specific to the context of a command.

- Mandatory Arguments
- Function-independent Arguments
- Function-dependant Arguments
- Function-specific Arguments
- Common Arguments
- Command Arguments

Mandatory Arguments

You must use the following arguments with all commands.

-u *userid*

Specifies the LMS username. You must define an environment variable `cwcli CWCLIFILE` with value set to a filename, which will contain the corresponding password.

The file has to be maintained by you. You can control the access permissions of this file to prevent un-authorized access. **cwcli config** looks for current working directory if `cwcli CWCLIFILE` is set to only file name instead of full path.

If **-u** argument is used along with **-p** argument, the password is taken from the command line instead of `cwcli CWCLIFILE`. This is not secure and usage of this argument is not recommended.

The password must be provided in the file in the following format:

```
username password
```

Where username is the LMS user name given in command line. The delimiter between username and password is single blank space. You must provide the delimiter if the password is blank

Otherwise, **cwcli config** will not validate the password. The password file can contain multiple entries with different user names. The password of the first match is considered in case of duplicate entries.

See Setting CWCLIFILE Environment Variable for more details.

Function-independent Arguments

You can use the following arguments without any commands:

-help

When run with the **-help** argument, **cwcli config** displays a list of all supported commands and a one-line description of the command.

-v

When run with the **-v** argument, **cwcli config** displays **cwcli config** version information.

Function-dependant Arguments

You can use the following arguments only with commands:

-p *password*

Specifies the password for the LMS username.

Warning **SECURITY WARNING: If -p *password* is used, the password is read from the command line instead of `cwcli CWCLIFILE`. This is highly insecure and *not* recommended. See -u argument for more details. See Setting CWCLIFILE Environment Variable for more details.**

`-d` *debuglevel*

Sets the debug level based on which debug information is printed. debuglevel is a numeric value between 1 and 5.

`-f` *filename*

Specifies the name of the file to which the retrieved configuration is written. If not specified, devicename.cfg is assumed.

`-l` *logfile*

Logs the results of the `cwcli config` command to the specified log filename.

`-m` *mailbox*

Mails the results of the `cwcli config` command to the specified email address.

Function-specific Arguments

You can use the following arguments only with specific commands:

`-baseline`

Used with the `compareanddeploy, deploycomplianceresults, listversions, createdeployparamfile, directbaselinedeploy,` or `comparewithbaseline function`, specifies the name of the Baseline template that is compared with the latest configuration version of the device.

If there are commands in the baseline configuration file that are not compliant with the latest configuration of the device in the archive, they are downloaded to the device.

Note The Baseline template must not contain any parameters for the command to succeed.

`-date` *date1 date2*

Used with the `compare` or `delete` command, specifies the configuration date(s) to compare or delete. Use the format mm/dd/yyyy.

`-device` *name*

Used with the `export, import,` or `put` function, specifies the name of the device. You can specify a wildcard, %, in the device name to match any device(s) that have the same textual pattern.

`-device` *list*

Used with the `get, start2run, compare, compareanddeploy, comparewithbaseline, deploycomplianceresults, listversions, put, run2start, start2run, write2run` or `delete` commands

Specifies the list of device names separated by commas. You can specify a wildcard, %, in the device list to match device(s) that have the same textual pattern.

`- ipaddress` *list*

Used with the `get, start2run, compare, compareanddeploy, comparewithbaseline, deploycomplianceresults, listversions, put, run2start, start2run, write2run` or `delete` commands.

Specifies IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated.

You cannot use this option with **-device**, **-view**, or **-input**. Also, you cannot specify wildcard characters.

-filetype *type*

Used with the put function, specifies the type of the configuration (running/vlan) that should be written to the device.

-f *filename*

Used with the **directbaselinedeploy, export, import, write2run or write2start function**, specifies the name of the file to which the configuration from archive should be exported to. Used with the **import** function, specifies the name of the file that contains the configuration to import.

Note **-f** argument must not be specified when **-view** or **-device** % is used. If used, the given file will be overwritten with the configuration retrieved for other devices.

-input *listfile*

Used with the **export, import, compareanddeploy, comparewithbaseline, deploycomplianceresults** or **put** function, specifies the name of the file containing the arguments for multiple devices.

The contents of the file must be similar to those described in the Input List File Format section later in this man page.

-listonly

Used with the **write2run** function, lists the differences between the running configuration and the specified configuration file.

-reboot

Used with the **import** or **put** function, reboots the device after the configuration has been written to the device.

-save

Used with the **import** or **put** function, saves the configuration written to the device to the device's memory.

-timeout

Used with the **compareanddeploy, deploycomplianceresults, import, put, run2start, start2run, write2run** or **comparewithbaseline** function, specifies the duration of the interval in seconds between two successive polling cycles.

-version number

Used with the **export** function, specifies the configuration version to retrieve from the archive. Used with the put function, specifies the configuration version to load from the archive and push to the device.

-version *version1 version2*

Used with the **compare**, or **delete** function, specifies the configuration version(s) to compare or delete.

-view *name*

Specifies the device view where the device name specified with **-device** argument is located. If **-device** argument is not specified, performs the operation on all devices in the view. More details are described in the **-view** Argument Usage section later in this man page.

-xml

Creates an XML file with the name of the device containing the configuration retrieved.

Input List File Format

For commands that do not accept multiple device names on the command line, such as put, **import**, and **export**, you can create an input list file that contains a list of devices to perform the operation on.

The contents of the input list file are a sequence of lines. Each line specifies a device name and the arguments to apply to that device. The arguments must be specific to the function. You cannot include view names in the input list file. You must specify view names on the command line. You can include comments in the input list file by starting the each commented line with #.

Input List File Example:

For the command

cwcli config put -u *userid* **-p** *password* **-view** *myView* **-input** ~/*todo_list*

An example of the input list file ~/todo_list is # Comment line.

```
-version 3 -reboot -device enm-2501.cisco.com
-version 2 -save -device enm-4500.cisco.com
```

-view Argument Usage

If both **-device** and **-view** are specified, the devices in that view and the devices specified against **-device** are considered.

For example, assume that **-view** has two devices D1 and D2 and D3 is specified against **-device**, then all the three devices D1, D2 and D3 are considered.

-view Argument Usage Examples:

Search for a device in a specified view:

cwcli config export -u *admin* **-p** *admin* **-view** *myView* **-device** *myDevice*

cwcli config Subcommand Man Pages

Each **cwcli config** command has a man page. You can access these man pages from the command line of a LMS server installed on a UNIX system.

To view the man pages, add the path:

install_dir/CSCOpx/man to the *MANPATH* variable.

Then you can enter the command
man cwc- *command*

where *command* is the command name. For example, export.

This topic contains the man pages for the following **cwcli config** subcommands:

- compare
- comparewithbaseline
- compareanddeploy
- delete
- deploycomplianceresults
- export
- get

- import
- put
- reload
- run2start
- start2run
- write2run
- write2start
- listversions
- createdeployparamfile
- directbaselinedeploy
- collectiondate
- accessdate

compare

Name	**cwcli config compare** – CiscoWorks **cwcli config compare** function
Syntax	**cwcli config compare -u** *userid* **-p password** [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* | **-ipaddress** *list* } { **-version** *version1* [*version2*] | **-date** *date1* [*date2*] } **cwcli config compare -help**
Description	**compare** lists the differences between versions of a device configuration. You can specify the versions to be compared by using the **-version** argument or the **-date** argument. • If you specify the **-version** argument with only one version number, that version is compared with the latest archived configuration of the device. • If you specify the **-date** argument with only one date, the configuration version with that date is compared with the latest archived configuration. When specifying a date, use the format mm/dd/yyyy. • If you do not specify either a date or a version, the latest two archived configurations are compared. You can specify multiple devices by separating each device name with a comma. The output of the Compare function can be interpreted as follows: – Lines preceded by '+' sign signify those occurring only in the first version but not in the latter. – Lines preceded by '-' sign signify those occurring only in the latter version but not in the first. – Lines preceded by '<' and '>' connote those which are present in both files but differ from each other.

compareanddeploy

Name	**cwcli config compareanddeploy** – CiscoWorks compare and download configuration with Baseline template function.
Syntax	**cwcli config compareanddeploy -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* }{ **-baseline** *baselinefile* }[**-timeout** *seconds*] [**-input** *argumentFile*] [**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*] **cwcli config compareanddeploy -help**
Description	**compareanddeploy** creates a job that compares the given Baseline template with the latest version of the configuration for a device and downloads the configuration to the device if there is non-compliance. If you specify **-baseline** argument, the name of the Baseline template is compared with the latest configuration version of the device and later downloaded to the device if there are any commands in the baseline config file which are not compliant with the latest configuration of the device in the archive. The Baseline template must not have any parameters for the command to succeed.

comparewithbaseline

Name	**cwcli config comparewithbaseline** - CiscoWorks compare configuration with Baseline template function.
Syntax	**cwcli config comparewithbaseline -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* }{ **-baseline** *baselinefile* }[**-timeout** *seconds*] [**-input** *argumentFile*] **cwcli config comparewithbaseline -help**
Description	**comparewithbaseline** creates a job that compares the given Baseline template with the latest version of the configuration for a device. If you use the **-baseline** argument, the name of the Baseline template is compared with the latest configuration version of the device.

delete

Name	**cwcli config delete** – CiscoWorks **cwcli config delete** function
Syntax	**cwcli config delete -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* | **-ipaddress** *list* } { **-version** *version1* [*version2*] | **-date** *date1* [*date2*] } **cwcli config delete -help**
Description	**delete** deletes the specified device configuration from the archive. You can use the **-date** argument or the **-version** argument to specify which configurations to delete. • If you specify two dates, all configurations archived between those two dates are deleted. • If you specify only one date, all configurations up to and including the configuration archived on that date are deleted. • If you specify two versions, all configurations between and including the two versions are deleted. • If you specify only one version, the configuration corresponding to that version is deleted.

deploycomplianceresults

Name	**cwcli config deploycomplianceresults** - CiscoWorks deploy command with baseline function.
Syntax	**cwcli config deploycomplianceresults -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-substitute** *datafile* } {**-jobid** *jobID*}[**-timeout** *seconds*][**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*] **cwcli config deploycomplianceresults -help**
Description	**deploycomplianceresults** uses the previously run **comparewithbaseline** job to get the non-compliance commands and creates a job after replacing the parameters if any in the non-compliance commands with the values from the data file and then downloads those commands to ensure the compliance with the baseline config. If you specify the **-baseline** argument, the name of the Baseline template which will be compared with the latest configuration version of the device.

export

Name	**cwcli config export** – CiscoWorks **cwcli config**'s **export** function.
Syntax	**cwcli config export -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *name* | **-view** *name* | **-device** *name* **-view** *name* |**-ipaddress** *list* } [**-f** *filename*] [**-version** *number*] [**-xml**] [**-input** *argumentFile*] **cwcli config export -help**
Description	**export** retrieves the configuration specified by the **-version** argument, for the device specified by **-device** and/or **-view** argument, from the archive and writes it to the file specified by the **-f** argument. • If you do not specify a version number, the latest configuration of the device from the archive is retrieved. • If you do not specify a file name, a file named devicename.cfg is created. To run this command against multiple devices, you must specify the **-input** argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of the **cwcli config** man page.

get

Name	**cwcli config get** – CiscoWorks **cwcli config** get function
Syntax	**cwcli config get -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] **-filetype** *running|startup|runningstartup* **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* | **-ipaddress** *list* } **cwcli config get -help**
Description	**get** retrieves the running configuration from the device(s), specified by the **-device** and/or **-view** argument, and pushes it to the configuration archive if the running configuration is different than the latest version in the archive. For devices that support vlan configuration like CatIOS devices, the vlan configuration is also fetched and archived along with running-configuration. However, if a new version of the running configuration is not archived, the vlan configuration fetched, overwrites the previously archived vlan configuration for the latest version of running configuration in the archive. You can run the get function against multiple devices by separating each device name with a comma.

import

Name	**cwcli config import** – CiscoWorks **cwcli config import** function
Syntax	**cwcli config import -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*][**-timeout** *time*] { **-device** *name* |**-ipaddress** *address*} [**-f** *filename*] [**-save** [**-reboot**]][**-input** *argumentFile*] **cwcli config import -help**
Description	**import** retrieves the configuration from a file specified by the **-f** argument, and pushes it to the device specified by the **-device** and/or the **-view** argument, adding to the device's running configuration. • If you do not specify a file name, a file named device name.cfg is used. You can specify the **-save** and **-reboot** arguments, which operate the same as for the put argument. To run the **import** argument against more than one device, you must specify the **-input** argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of **cwcli config**(1). The configuration archive might be updated after you specify the **import** argument if the loaded configuration is different from the latest configuration in the archive.

put

Name	**cwcli config put** – CiscoWorks **cwcli config** put function
Syntax	**cwcli config put -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *name* |**-ipaddress** *address* **-version** *number*}[**-config** *1|2*][**-save** [**-reboot**]] [**-input** *argumentFile*][**-timeout** *seconds*] [**-filetype** *vlan|running*][**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*]] **cwcli config put -help**
Description	**put** retrieves the configuration specified by **-version** from the configuration archive and pushes it to the device specified by the **-device** and/or **-view** argument The **-filetype** can be used to specify the type of configuration viz running/vlan configuration. By default, the running configuration is considered • In case of running configuration, the archived running configuration is merged with the running configuration on the device unless you specify **-save**, in which case, the archived configuration is also written to the device's memory. • In case of vlan configuration, the archived vlan configuration overwrites that on the device. The vlan configuration will not come into effect until the device is rebooted. You can specify **-reboot** to reboot the device after the configuration (running/vlan) is pushed to the device. To run the put command on more than one device at a time, you must use the **-input** argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of **cwcli config**(1).

reload

Name	**cwcli config reload** – CiscoWorks **cwcli config reload** function
Syntax	**cwcli config reload -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name*|**-ipaddress** *list* }[**-input** *argumentFile*][**-timeout** *seconds*][**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*] **cwcli config reload -help**
Description	**reload** reboots the device(s), specified by the **-device** and/or **-view** argument, resulting in the running configuration being loaded with its startup configuration. You can specify multiple devices with the **-device** argument by separating each device name with a comma.

run2start

Name	**cwcli config run2start** – CiscoWorks **cwcli config run2start** function
Syntax	**cwcli config run2start -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*]{ **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* | **-ipaddress** *list*}[**-config** *1*|*2*] [**-input** *argumentFile*][**-timeout** *seconds*][**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*] **cwcli config run2start -help**
Description	**run2start** overwrites the startup configuration of any device(s), specified by the **-device** and/or **-view** argument, with its running configuration. You can specify multiple devices with the **-device** argument by separating each device name with a comma or with the **-input** argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of **cwcli config**(1).

start2run

Name	**cwcli config start2run** – CiscoWorks **cwcli config start2run** function
Syntax	**cwcli config start2run -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* | **-ipaddress** *list* } [**-config** *1*|*2*] [**-input** *argumentFile*][**-timeout** *seconds*] [**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*] **cwcli config start2run -help**
Description	**start2run** merges the running configuration of any device(s), specified by the **-device** and/or **-view** arguments, with its startup configuration to give a new running configuration. You can specify multiple devices with the **start2run** argument by separating each device name with a comma or with the **-input** argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of **cwcli config**(1).

write2run

Name	**cwcli config write2run –** CiscoWorks **cwcli config write2run** function
Syntax	**cwcli config write2run -u** *userid* **-p** *password* [**-d** *debuglevel*][**-m** *email*][**-l** *logfile*] { **-device** *name* | **-ipaddress** *address*} **-f** *filename* [**-config** *1|2*][**-listonly**][**-input** *argumentFile*][**-timeout** *seconds*][**-primary_user** *primary user name*][**-primary_pass** *Base64 encoded primary password*][**-enable_pass** *Base64 encoded enable password*] **cwcli config write2run -help**
Description	**write2run** compares the latest running configuration for the device in the configuration archive with the configuration in the file specified by the **-f** argument to generate a new configuration that is downloaded to the device, so that the end result is that the configuration specified in the file is available on the running configuration of the device. If **-listonly** is specified, the difference between the latest running configuration for the device in the configuration archive and the new configuration that is generated is listed on the display, but no configuration is downloaded to the device. To run this command against multiple devices, specify the **-input** argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of **cwcli config**(1). **CAVEAT** This command is not 100% reliable in that it may not successfully overwrite the running configuration. This is due to the dependency on the underlying Diff API, which generates the configuration difference to be downloaded to the device to make the running configuration on the device same as the one specified in the file (by the **-f** argument).

write2start

Name	**cwcli config write2start –** CiscoWorks **cwcli config write2start** function
Syntax	**cwcli config write2start -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *name* **-f** *filename* |**-ipaddress** *address*} [**-config** *1|2*][**-input** *argumentFile*][**-timeout** *seconds*][**-primary_user** *primary user name*][**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*] **cwcli config write2start -help**
Description	**write2start** erases the contents of the device's startup configuration and then writes the contents of the given file as the device's new startup configuration. If you do not specify a file name, it prints an error message and exits. To run this command against multiple devices, you must specify the **-input** argument, which takes a file name as its argument. The contents of the file must be similar to those described in the Input List File Format section of **cwcli config**(1).

listversions

Name	**cwcli config listversions –** CiscoWorks **cwcli config listversions** function
Syntax	**cwcli config listversions -u** *userid* **-p password** [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*]{ **-device** *name* | **-view** *name* | **-device** *name* **-view** *name* | **-ipaddress** *list*} [**-baseline**][**-input** *argumentFile*] **cwcli config listversions -help**
Description	**Listversions** (specified by "listversions") lists the different versions of configuration files archived in the archival system. If you use the **-baseline** argument, only the names of the Baseline templates are displayed. You can choose a template and use it inline with the **comparewithbaseline** and **compareanddeploy** commands.

createdeployparamfile

Name	**cwcli config createdeployparamfile -** CiscoWorks **cwcli config createdeployparamfile** function.
Syntax	**cwcli config createdeployparamfile -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*][**-jobid** *comparewithbaseline jobid*] [**-baseline** *baselinefile*] [**-f** *parameterfile*] **cwcli config createdeployparamfile -help**
Description	**createdeployparamfile** creates a parameter file if the Baseline template containing the parameters is specified. You can use the **-jobid** argument to specify the job identifier of the previously executed **comparewithbaseline** job. You can choose a template with the **-baseline** argument and specify the name of the Baseline template for which the parameter file has to be created.

directbaselinedeploy

Name	**cwcli config directbaselinedeploy -** CiscoWorks **cwcli config directbaselinedeploy** function
Syntax	**cwcli config directbaselinedeploy -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-baseline** *baselinefile* } {**-substitute** *parameterfile*}[**-timeout** *seconds*] [**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*] **cwcli config directbaselinedeploy -help**
Description	**directbaselinedeploy** creates a job that downloads the given Baseline template after retrieving the values of the parameters in the template from the given parameter file. You can use the **-timeout** argument to specify the duration of the interval in seconds between the two successive polling cycles. You can use the **-baseline** to specify the name of the Baseline template which will be compared with the latest configuration version of the device and later downloaded to the device if there are any commands in the baseline config file which are not compliant with the latest configuration of the device in the archive. You can use the **-substitute** to substitute the values from the XML parameter file for the parameters specified in the template.

collectiondate

Name	`cwcli config collectiondate` - CiscoWorks `cwcli config collectiondate` function
Syntax	`cwcli config collectiondate -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*] [`-l` *logfile*] [`-filetype` *running*|*startup*|*vlan*] [`-input` *argumentFile*] { `-device` *list* `-view` *name* |`-ipaddress` *list* } `cwcli config collectiondate -help`
Description	`collectiondate` displays the last config collection date for the devices. The output contains device name, time of last config collection, and the filetype separated by comma.

accessdate

Name	`cwcli config accessdate` - CiscoWorks `cwcli config accessdate` function
Syntax	`cwcli config accessdate -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*] [`-l` *logfile*] [`-filetype` *running*|*startup*|*vlan*] [`-input` *argumentFile*] { `-device` *list* `-view` *name* |`-ipaddress` *list* } `cwcli config accessdate -help`
Description	`accessdate` displays the last config collection attempt date for the devices. The output contains device name, time of last attempt, and the filetype separated by comma.

Overview: cwcli netconfig Command

The `cwcli netconfig` command lets you use NetConfig from the command line.

This section contains cwcli netconfig Remote Access.

Caution The `cwcli netconfig` command does not validate the command arguments you use or the configuration commands that you run using it. If you enter incorrect commands you can misconfigure or disable the devices on which the job runs.

Running the cwcli netconfig Command

To use the `cwcli netconfig` command, you must be able to run the cwcli command, and you must have permissions to use the Adhoc system-defined task. For more details see topic in the section.

The command syntax is:

`cwcli netconfig` *Sub_command Common_arguments Command_arguments*

The subcommands and arguments are described in the following sections:

- Subcommands (see Subcommands)
- Common Arguments (see Common Arguments)
- Command Arguments (see Command Arguments)

Subcommands

Subcommands specify the action the command performs. Valid values for the subcommands are:

Sub Command	Description
createjob	Creates job.
deletejob	Deletes jobs.
canceljob	Cancels jobs.
jobdetails	Lists job details.
jobresults	Lists job results.
`listjobs`	Lists jobs.
`import`	Imports user-defined tasks in XML format.
`export`	Exports user-defined tasks in XML format.
`listtasks`	Lists the NetConfig user-defined tasks.

Common Arguments

Common arguments specify parameters that apply to all subcommands. Valid values for common_arguments are:

Command Argument	Description	Usage Notes
`-u` *user*	Enter valid CiscoWorks username.	None
`-p` *password*	Enter password for username. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.	None

Command Arguments

Command arguments specify parameters that apply only to specific subcommands.

The conventions followed are:

- Arguments in [ ] are optional. For optional arguments, if you do not specify a value the default value that has been set by the administrator using the NetConfig UI, will become applicable.
- Arguments in { } denote that you must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).
- Arguments suffixed with + denote that you can enter multiple values separated with spaces.
- Values that contain spaces need to be entered within “ ”. For example, the job description that you provide when you use a the `createjob` command should be entered within “ ”.

Valid values for command_arguments are described in the following table:

Sub Command	Command Argument	Description	Usage Notes
createjob Allows you to create a NetConfig job.	{**-device** *comma_separated_device_names* | **-devicefile** *devicelist_filename* | **-view** *device_view_name*}	Defines devices to be configured. *comma_separated_device_names* is list of device display names. *devicelist_filename* is path to device list file. Can be full pathname or filename in the local directory. The devicelist file should be of this format: **-device** 1.1.1.1,2.2.2.2,3.3.3.3 or **-device** 1.1.1.1 **-device** 2.2.2.2 **-device** 3.3.3.3 *device_view_name* is name of the device view.	Jobs can run only one device category (IOS, Catalyst, Content Engine (CE), or Content Service Switch (CSS)). Do not enter devices of multiple categories.
	{[{**-commandfile** *commandlist_filename* **-mode** {config | enable}} [**-rollbackfile** *rollback_cmdlist_filename*]] [**-taskname :** "*User defined task name*"]}	Defines configuration commands to be used. You can specify the command file path, the command mode, the rollback file and the name of the user-defined task. Specify the user-defined task name within quotes.	*commandlist_filename* is path to command file. Can be a full pathname or filename in local directory. **-mode** specifies the command mode.{config | enable} are the command mode arguments. By default, **-mode** value is set to config. This is not valid for jobs that configure Catalyst devices. For jobs on IOS, CE, or CSS devices, config is default. *rollback_cmdlist_filename* defines the rollback configuration commands for the job. It can be a full pathname to the file or a filename in the local directory. *User defined task name* is the name that you specify for the user-defined task.
	{**-description :** *"job_description "*}	Enter the description for the job you are creating.	*"job_description"* is the description you specify, for the job that you are creating. Enter this value within quotes.

Sub Command	Command Argument	Description	Usage Notes
	[{`-schedule` : *MM/dd/yyyy:HH:mm:ss* `-schedule_type`: `once`| `weekly`| `monthly`| `lastDayOfMonth`}]	`-schedule` defines time and date job will run. If you have enabled Job Approval, and later if you create the job without using the `-schedule` argument, the job will automatically be scheduled to run after 5 minutes of the job creation time. You should approve this job within 5 minutes of creating the job. If you want to schedule the job to run at any other time, use the `-schedule` argument. If not specified, job will run immediately. `-schedule_type` defines the type of job schedule.	*MM* is month (01 to 12). *DD* is day of month (01 to 31). *YYYY* is year (Example: 2004). *HH* is hours, *mm* is minutes, and *ss* is seconds in 24-hour time. If you do not specify the schedule type, the job will be an immediate job.
	[`-policyfile` *policy_filename*]	Defines job policies using a job policy file. You can specify job policies using combination of `-policyfile` argument and other optional arguments, However, you can specify each argument only once in command.	*policy_filename* is path to job policy file. Can be a full pathname or filename in local directory.
	[`-makercomments` : *"maker comments"*]	Comments from the job creator, to the job approvers, if job approval is enabled for the job.	Enter your comments within quotes.
	[`-mkemail` : *maker email id*]	E-mail ID of the job creator, for approval notifications, if approval is enabled for the job.	None
	[`-execution`: `Sequential`|`Parallel`]	Configures the job execution property, whether the jobs should be run sequentially or in parallel.	None.
	[`-startup`]: Copy running config to startup policy	Select to cause the configuration job to write the running configuration to the startup configuration on each device after configuration changes are made successfully.	None.

Sub Command	Command Argument	Description	Usage Notes
	[`-version`] : Fail on mismatch of Config Versions.	Select to cause the job to be considered a failure when the most recent configuration version in the Configuration Archive is not the same as the configuration that was running when you created the job.	`-sync` argument should be provided if this policy is selected. This argument causes the job to archive the running configuration before making configuration changes.
	[`-email` : *Job Notification email ids*]	Specify the email addresses to which the configuration job will send status notices.	Separate multiple addresses with commas.
	[`-sync`] : Synch configuration archive before deploy	Select to cause the job to archive the running configuration before making configuration changes.	None.
	[`-failure`: "`Stop on failure`" | "`Ignore failure and continue`" | "`Rollback device and stop`" | "`Rollback device and continue`" | "`Rollback job on failure`"]	Select what the job should do if it fails to run on a device.	Ensure that you place your selected value within quotes.
	[{`-primary_user` : *Primary User name* `-primary_pass` : "*Primary password*" }]	Primary username for connecting to the device. Primary password for connecting to the device.	Enter the primary password within quotes.
	[`-enable_pass` : "*Execution mode Password*"}]	Password for running commands in the execution mode, on the device.	Enter the execution mode password within quotes.
`deletejob` This subcommand allows you to delete one or more NetConfig jobs.	`-id` *job_id+*		*job_id+* specifies the ID of the job on which to act. You can specify multiple job IDs separated by spaces or commas.
canceljob This subcommand allows you to cancel a NetConfig job from the command line.	`-id` *job_id*		*job_id* specifies ID of job on which to act.
jobdetails Allows you to view details of one or more NetConfig jobs from the command line.	[`-id` *job_id+*]	Specifies ID of job on which to act.	You can specify multiple job ID separated by spaces or commas.

Sub Command	Command Argument	Description	Usage Notes
jobresults Allows you to view results of one or more NetConfig jobs from the command line.	[**-id** *job_id+*]	Specifies ID of job on which to act.	You can specify multiple job ID separated by spaces or commas.
	[**-details**]	Specifies full details of job results to be displayed.	Not specifying details will display only the summary of job execution result.
listjobs Allows you to list all NetConfig jobs from the command line.	[**-status {A(ll)** | **R(unning)** | **C(ompleted)** | **P(ending)**}]	Specifies status of jobs to list.	If status is not specified, all registered jobs are listed.
import Allows you to import user defined task in xml format to to netconfig from the command line.	{**-taskfile** *User-defined task file* }	User-defined task filename in XML format.	
export Allows you to export one or more user defined tasks created in netconfig to xml files from the command line.	{ **-task+** *User-defined task name* }	Name of the user-defined task to be exported.	You can specify multiple tasks separated by spaces or commas.
	{**-dest** *file export location* }	Path of the destination location to which the exported user-defined task file is to be copied.	
listtask		Lists the NetConfig user-defined tasks.	

Command Examples

Example 1

The command

cwcli netconfig createjob -u *username* **-p** *password* **-devicefile** *devicefile* **-commandfile** *command.file* **-failure** *Ignore failure and Continue* **-startup**

creates a NetConfig job with the following characteristics:

- Devices mentioned in *devicefile* will be configured.
- Commands in file *command.file* will run.
- Job will continue if it fails to successfully configure a device.
- Each device's running configuration will be copied to startup as soon as the device is successfully configured.
- Job will run immediately because the **-schedule** argument is not specified.

Example 2

The command

cwcli netconfig createjob -u *username* **-p** *password* **-devicefile** *devicefile* **-commandfile** *command.file* **-policyfile** *policyfile*

creates a NetConfig job with the following characteristics:

- Devices listed in the file *devicefile* will be configured.
- Commands in the file *command.file* will run.
- The file *policyfile* contains job policy arguments that determine the job policy.

Understanding cwcli netconfig Input Files

Several types of text files are available for you to use as input for the **cwcli netconfig** command and the **-createjob** subcommand. You can also use the command list type as input for user-defined tasks.

File Type	Description	Usage Notes
Device list	Lists devices on which job will run. It lists one device on each line.	Use with **-devicefile** argument. Job can run only one device category (IOS, or Catalyst). Do not list devices of multiple categories.
Command list	Lists configuration commands that job will run; one command per line.	Use with **-commandfile** argument, or to add commands to a user-defined task.
Job policy	Lists of job policy arguments; one argument per line.	Use with **-policyfile** argument.

Examples

Device List File

```
-device device_display_name1
-device device_display_name2
-device device_display_name3
-device device_display_name4
```

Command List File

```
command1
command2
command3
command4
```

Job Policy File

This file configures the job to stop running if the job fails on a device, to write the running configuration to startup after configuration changes are made.

```
-failure Stop on Failure
-sync
```

cwcli netconfig Man Page Examples

On UNIX, you can view the complete man pages by setting the MANPATH to /opt/CSCOpx/man

The following are some examples from the NetConfig man page:

Examples

Device List File Example

For the command

cwcli netconfig createjob -u *userid* **-p** *password* **-devicefile** *c7000.dev* **-commandfile** *command.file*

-description *"cwcli netconfig job"* **-mode** config

An example of the device list file c7000.dev is

```
enm-7000-1.cisco.com
enm-7000-2.cisco.com
enm-7000-3.cisco.com
enm-7000-4.cisco.com
```

Command List File Example

For the command

cwcli netconfig createjob -u *userid* **-p** *password* **-devicelist** *c7000-1,c7000-2* **-commandfile** *command.file*

-description *"cwcli netconfig job"* **-mode** config

An example of the command file command.file is

```
snmp-server community public ro
snmp-server community private rw
```

Policy File Example

For the command

cwcli netconfig createjob -u *userid* **-p** *password* **-devicefile** *c7000.dev* **-commandfile** *command.file* **-policyfile** *policy.in*

-description *"cwcli netconfig job"* **-mode** config

An example of the policy file policy.in is

-failure *"Stop on failure"*

-sync

-execution Parallel

User-defined Task XML file Example

```
<?xml version="1.0" encoding="UTF-8"?>
<Task name="SampleTASK">
<Template mode="1" name="iproute" parameterized="false">
<Commands>
<cli>ip route 0.0.0.1 0.0.0.0 Ethernet0/0</cli>
<cli>ip route 0.0.0.2 0.0.0.0 Ethernet0/0</cli>
<cli>ip route 0.0.0.3 0.0.0.0 Ethernet0/0</cli>
```

```
<cli>ip route 0.0.0.4 0.0.0.0 Ethernet0/0</cli>
<cli>ip route 0.0.0.5 0.0.0.0 Ethernet0/0</cli>
<cli>ip route 0.0.0.6 0.0.0.0 Ethernet0/0</cli>
</Commands>
<RollbackCommands>
<cli>no ip route 0.0.0.4 0.0.0.0 Ethernet0/0</cli>
<cli>no ip route 0.0.0.5 0.0.0.0 Ethernet0/0</cli>
</RollbackCommands>
<MDFIds>268438030,273153536,272819655</MDFIds>
</Template>
</Task>
```

cwcli netconfig Remote Access

You can also perform the **cwcli netconfig** tasks using the servlet. You will have to upload a payload XML file, which contains the **cwcli netconfig** command arguments and LMS user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to run any command:

For post request,

perl *samplepost.pl* **http://***lms-server:lms-port***/rme/cwcli** *payload_XML_file*

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

perl *samplepost.pl* **https://***lms-server:lms-port***/rme/cwcli** *payload_XML_file*

The default port for LMS server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>
<command>
cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...
</command>
</payload>
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

For get request,

http://<rme-server>:<rme-port>/rme/cwcli?command=cwcli netconfig *commandname* **-u** *user* **-p** *BAse64 encoded pwd -args1 arg1value...*

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

https://*lms-server:lms-port***/rme/cwcli?command=cwcli netconfig** *commandname* **-u** *user* **-p** *BAse64 encoded pwd -args1 arg1value...*

The default port for LMS server in HTTPS mode is 443.

The BAse64 encoded for “admin” is YWRtaW4=.

The URL encode for,

- Double quotes (“) is %22
- Percentage sign (%) is %25

Overview: cwcli export Command

`cwcli export` is a command line tool that also provides servlet access to inventory, configuration and change audit data.

This can be used for generating inventory, configuration archive, and change audit data for devices in LMS.

This section contains:

Note You cannot run this command for the devices that are in Conflicting or Suspended state.

This tool supports the following features:

- Generating change audit data in XML format

  The tool uses the existing Change Audit log data and generates the Change Audit log data in XML format.

  See Running cwcli export changeaudit for the usage and XML schema details

- Generating configuration data in XML format

  The tool uses existing configuration archive APIs and generates latest configuration data from the configuration archive in XML format.

  Elements in the XML file are created at the configlet level in the current configuration archive. Predefined rules that currently exist in the configuration archive are used to get the configlets data.

  See Running cwcli export config for the usage and XML schema details

- Generating inventory data in XML format

  The tool has servlet access and command line utilities that can generate inventory data for devices managed by the LMS server.

  See Running cwcli export inventory Command for the usage and XML schema details

The **cwcli export** command is located in the following directories, where *install_dir* is the directory in which LMS is installed:

- On UNIX systems, /opt/CSCOpx/bin
- On Windows systems, *install_dir*\CSCOpx\bin

  The default install directory is C:\Program Files.

If you install LMS on an NTFS partition on Windows, only users in the administrator or casuser group can access **cwcli export**. Users with read-write access to the CSCOpx\files\archive directory and the directories under that can also use **cwcli export**.

You can also perform the **cwcli export** tasks using the servlet. You will have to upload a payload XML file, which contains the **cwcli export** command arguments and LMS user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to run any command:

For post request,

perl *samplepost.pl* **http://***lms-server:lms-port***/rme/cwcli** *payload_XML_file*

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

perl *samplepost.pl* **https://***lms-server:lms-port***/rme/cwcli** *payload_XML_file*

The default port for LMS server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>
<command>
cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...
</command>
</payload>
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

For get request,

http://*lms-server:lms-port***/rme/cwcli?command=cwcli export** *commandname* **-u** *user* **-p** *BAse64 encoded pwd -args1 arg1value...*

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

https://*lms-server:lms-port***/rme/cwcli?command=cwcli export** *commandname* **-u** *user* **-p** *BAse64 encoded pwd -args1 arg1value...*

The default port for LMS server in HTTPS mode is 443.

The BAse64 encoded for “admin” is YWRtaW4=.

The URL encode for,

- Double quotes (“) is %22 and Percentage sign (%) is %25

Using the cwcli export Command

The command line syntax of the application is in the following format:

cwcli export *command GlobalArguments AppSpecificArguments*

- **cwcli export** is the CiscoWorks command line interface for exporting inventory/config/changeaudit details into XML format.
- *Command* specifies which core operation is to be performed.
- *GlobalArguments* are the additional parameters required for each core command.
- *AppSpecificArguments* are the optional parameters, which modify the behavior of the specific **cwcli export** core command.

The order of the arguments and arguments are not important. However, you must enter the core command immediately after **cwcli export**.

The following sections describe:

- The **cwcli export** commands (See cwcli export Commands)
- The mandatory and optional arguments (See cwcli export Global Arguments)
- The default archiving location (See Archiving cwcli export Data in XML File)

On UNIX, you can view the **cwcli export** man pages by setting the MANPATH to /opt/CSCOpx/man.

The commands to launch the **cwcli export** man pages are:

- **man cwcli-export**—To launch the **cwcli export** command man page.
- **man export-changeaudit**—To launch the **cwcli export changeaudit** command man page.
- **man export-config**—To launch the **cwcli export config** command man page.
- **man export-inventory**—To launch the **cwcli export inventory** command man page.

cwcli export Commands

The following table lists the command part of the **cwcli export** syntax.

Command	Description
cwcli export changeaudit	Generates Change Audit log data in XML format.
cwcli export config	Generates configlets in XML format
cwcli export inventory	Generates Inventory data in XML format.

You must invoke the **cwcli export** command with one of the core commands specified in the above table. If no core command is specified, **cwcli export** can execute the **-v** or **-h**. arguments only. Argument **-v** specifies the version of the **cwcli export** utility and argument **-h** (or null argument) displays the usage information of this tool.

cwcli export Global Arguments

The following describes the mandatory and optional global arguments for **`cwcli export`**:

Global Arguments	Description
`-u` *userid*	Mandatory Specifies the LMS username.
`-p` *password*	Mandatory Specifies the password for the LMS username. If you want to avoid the **`-p`** argument which will reveal the password in clear text in cli, you will have to store your username and password in a file and set a variable `cwcli` *`CWCLIFILE`* which points to the file. You will have to maintain this file and control access permissions to prevent unauthorized access. **`cwcli export`** looks for current working directory if `cwcli` *`CWCLIFILE`*is set only to file name instead of full path. If you use the **-p** argument, even after setting the `cwcli` *`CWCLIFILE`* variable the password is taken from the command line instead of `cwcli` *`CWCLIFILE`*. This is not secure and usage of this argument is not recommended. The password must be provided in the file in the following format: username password where username is the LMS user name given in the command line.The delimiter between the username and password is single blank space. You must enter the delimiter if the password is blank. Otherwise, **`cwcli export`** will fail to validate the password.The password file can contain multiple entries with different user names. The password that matches first is considered in case of duplicate entries. **Note** If `-p` *password* is used, the password is read from the command line instead of `cwcli` *`CWCLIFILE`*. This is highly insecure and therefore not recommended. See Setting CWCLIFILE Environment Variable for more details.
{ **`-device`** *devicename* | **`-view`** *viewname*| **`-input`** *inputfilename* | **`-ipaddress`** *mgmt-ip-address* }	Mandatory **`-device`** *devicename* Specifies the display name of the device that you have added in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices). You can enter multiple display name separated by a comma. You can use either wildcard or specific device(s) but not at the same time. The argument syntax used for **`-device`** argument may be a single device or a device list. Devices in a list are separated by a '**,**'. The wild card symbol '**%**' may be used to specify a group of devices having a pattern. For example if a pattern ***x*%** is specified as a device in the list, then all the LMS devices that have names that start with x will be selected for this operation.

Global Arguments	Description
{ **-device** *devicename* | **-view** *viewname* | **-input** *inputfilename* | **-ipaddress** *mgmt-ip-address*}	Mandatory **-view** *viewname* If the data needs to be generated for all the devices in a specific group, you can use the **-view** argument. You can use this argument to generate data for devices in all device views including system-defined groups and user-defined groups. You can enter multiple group name separated using a comma. For view name, you have to enter the fully qualified path as in the Group Administration window. To separate the path you must use forward slash only. For example, **-view** "/RME@*ciscoworks_servername*/All Devices"
{ **-device** *devicename* | **-view** *viewname* **-input** *inputfilename* | **-ipaddress** *mgmt-ip-address*}	Mandatory **-input** *inputfilename* You can create an input list file that contains a list of devices to perform the operation on. The contents of the input list file are a sequence of lines. Each line specifies a display name as entered in the Device and Credential Repository. The arguments must be specific to the function. You cannot include group names in the input list file. You can include comments in the input list file by starting each commented line with #. The input file should be of this format: **-device** 1.1.1.1,2.2.2.2,3.3.3.3 or **-device** 1.1.1.1 **-device** 2.2.2.2 **-device** 3.3.3.3
{ **-device** *devicename* | **-view** *viewname* **-input** *inputfilename* | **-ipaddress** *mgmt-ip-address*}	Mandatory **-ipaddress** *mgmt-ip-address* Specify the device IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated. You cannot use this option with **-device**, **-view**, or **-input**. Also, you cannot specify wildcard characters.
-d *debuglevel*	Optional *debug_level* is a number between 1 (the least information is sent to the debug output) and 5 (the most information is sent to the debug output). If you do not specify this argument, 4(INFO) is the default debug level.
-l *logfile*	Optional Logs the results of the **cwcli export** command to the specified log file name. By default the command output will be displayed on the standard out.

Global Arguments	Description
`-m` mailid	Optional Mails the results of the `cwcli export` command to the specified email address. This argument notifies you whether the task is completed. Only one mail id can be given at a time.
`-f` *filename*	This is applicable only for changeaudit and inventory applications. Optional Specifies the name of the file to which the changeaudit and inventory information is to be exported on LMS server. If you are using `cwcli` remotely (get or post request), by default the output file is available at this location on LMS server: On Windows: *NMSROOT*\MDC\tomcat Where, *NMSROOT* is the LMS installed directory. On Solaris and Soft Appliance: *NMSROOT*/objects/dmgt

Archiving cwcli export Data in XML File

By default, the data generated through `cwcli export` command is archived at the location:

cwcli export *Command*	Location on LMS Server
changeaudit	On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/archive/*YYYY-MM-DD-HH-MM-SS* -changeaudit.xml
	On Windows: *NMSROOT*\files\rme\archive*YYYY-MM-DD-HH-MM-SS* -changeaudit.xml
config	On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/cwconfig/*YYYY-MM-DD-HH-MM-SS-MSMS MS-Device_Display_Name*.xml
	On Windows: *NMSROOT*\files\rme\cwconfig*YYYY-MM-DD-HH-MM-SS-MSMSMS -Device_Display_Name*.xml
inventory	On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/archive/*YYYY-MM-DD-HH-MM-SS*-inventory .xml
	On Windows: *NMSROOT*\files\rme\archive*YYYY-MM-DD-HH-MM-SS*-inventory.xml

Where *NMSROOT* is the LMS installed directory.

You can also specify a directory to store the output. This application does not have a feature to delete the files created in the archive. You should delete the files when necessary.

While generating data through the servlet, the output will be displayed in the client terminal.

Running cwcli export changeaudit

Using this command you can export the Change Audit log data in the XML format.

The command syntax for **cwcli export changeaudit** is:

cwcli export changeaudit {**-u** *username* **-p** *password* **-device** *devicenames*}
[**- ipaddress** *mgmt-ip-address*]

[**-f** *filename*]

[**-from** *mm/dd/yyyy*] ---> eg: 05/01/2004

[**-to** *mm/dd/yyyy*] ---> eg: 05/06/2004

[**-app** *comma separated list of applications*]

[**-cat** *comma separated list of categories*]

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you enter an argument which has space then use double quotes for that argument. For example for Software Management, you enter this as “Software Management”.

The following table describes the arguments that are specific to **cwcli export changeaudit** command. The other common arguments used by **cwcli export** are explained in Using the cwcli export Command.

Arguments	Description
[**-from** *mm/dd/yyyy*]	Optional. Enter the from date. If you enter only **-from** date then the report will be generated from the date that you have specified, to the current date.
[**-to** *mm/dd/yyyy*]	Optional. Enter the from date. If you enter only **-to** date then the report will be generated from the date LMS has logged Change Audit record to the **-to** date that you have specified.

Arguments	Description
[**-app** *comma separated list of applications*]	Specify the application name. The supported applications are: • Archive Mgmt • ConfigEditor • CwConfig • ICServer • NetConfig • Software Management If you do not specify the **-app** argument, then changes made by all applications is reported.
[**-cat** *comma separated list of categories*]	Specify the category name. The supported categories are: • CONFIG_CHANGE—Configuration changes on the device. • INVENTORY_CHANGE—Hardware changes on the device. • SOFTWARE_CHANGE—Software changes on the device. If you do not specify the **-cat** argument, then changes made by all categories is reported.

Note If you do not enter **-from** and **-to** arguments, all the Change Audit records logged till the current date will be displayed.

The following sections describes:

- XML Schema for cwcli export changeaudit
- XML Schema for Configuration Management Application
- XML Schema for Software Management
- Usage Examples for cwcli export changeaudit Command

XML Schema for cwcli export changeaudit

The following is the schema used for exporting the change audit data in XML format.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<!--Generated by XML Authority. Conforms to w3c http://www.w3.org/2000/10/XMLSchema-->
<xsd:schema xmlns:xsd = "http://www.w3.org/2000/10/XMLSchema">
 <xsd:element name = "changeRecord">
  <xsd:complexType>
   <xsd:sequence>
    <xsd:element ref = "groupId"/>
    <xsd:element ref = "category"/>
    <xsd:element ref = "host"/>
    <xsd:element ref = "user"/>
    <xsd:element ref = "device"/>
    <xsd:element ref = "connectionMode"/>
    <xsd:element ref = "timestamp"/>
    <xsd:element ref = "description"/>
   </xsd:sequence>
   <xsd:attribute name = "id" use = "required" type = "xsd:integer"/>
  </xsd:complexType>
```

```
 </xsd:element>
 <xsd:element name = "groupId" type = "xsd:string"/>
 <xsd:element name = "category" type = "xsd:string"/>
 <xsd:element name = "application" type = "xsd:string"/>
 <xsd:element name = "host" type = "xsd:string"/>
 <xsd:element name = "user" type = "xsd:string"/>
 <xsd:element name = "device" type = "xsd:string"/>
 <xsd:element name = "connectionMode" type = "xsd:string"/>
 <xsd:element name = "timestamp" type = "xsd:string"/>
 <xsd:element name = "description">
  <xsd:complexType>
   <xsd:sequence>
    <xsd:element ref = "summary"/>
    <xsd:element ref = "details"/>
   </xsd:sequence>
  </xsd:complexType>
 </xsd:element>
 <xsd:element name = "summary" type = "xsd:string"/>
 <xsd:element name = "details">
  <xsd:complexType/>
 </xsd:element>
 <xsd:element name = "changeRecordSet">
  <xsd:complexType>
   <xsd:sequence>
    <xsd:element ref = "changeRecord" maxOccurs = "unbounded"/>
   </xsd:sequence>
  </xsd:complexType>
 </xsd:element>
</xsd:schema>
```

Detailed Description of changeaudit Schema

The table below describes elements in the changeaudit schema:

Field	Description
Category	Type of the change. For example, configuration, inventory, or software.
Application	Name of the LMS application involved in the network change (Device Configuration, Inventory, or Software Management).
Host	Host device from which the user accessed the device or the host name of the LMS server.
User	Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the LMS is running, or the name under which the Telnet connection is established.
Device	Network device on which the change occurred. The display name as entered in the Device and Credential Repository.
ConnectionMode	Connection mode through which the change was made, for example, Telnet, snmp, console, or LMS.

Field	Description
Timestamp	Date and time at which the application communicated the network change or when Change Audit saw the change record.
Description	Contains the detailed information of the changes that had occurred on the device. The description changes based on the application you have selected: • Archive Mgmt (See XML Schema for Configuration Management Application for more information.) • ConfigEditor (See XML Schema for Configuration Management Application for more information.) • CwConfig (See XML Schema for Configuration Management Application for more information.) • ICServer—Inventory Collection Service (See XML Schema for Inventory Collection Service for more information.) • NetConfig (See XML Schema for Configuration Management Application for more information.) • Software Management (See XML Schema for Software Management for more information.)

The following section describes the schema used by these application when you run the command **`cwcli export changeaudit`** with **`-app`** argument:

- Archive Mgmt, ConfigEditor, CwConfig, NetConfig
- Inventory Collection Service
- Software Management

XML Schema for Configuration Management Application

The following XML schema is used by all Configuration Management application when you run the **`cwcli export changeaudit`** command with **`-app`** argument and the **`-app`** argument values as either *Archive Mgmt*, *ConfigEditor*, *CwConfig*, or *NetConfig*.

The schema file is:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--  edited with XMLSPY v2004 rel. 2 U (http://www.xmlspy.com) by Cisco (t) -->
- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
    - <xs:element name="ConfigDiff">
        - <xs:annotation>
            <xs:documentation>Comment describing your root element</xs:documentation>
          </xs:annotation>
        - <xs:complexType>
            - <xs:sequence>
                - <xs:element name="OldConfig">
                    - <xs:complexType>
                        - <xs:sequence>
                            <xs:element name="Command" maxOccurs="unbounded" />
                        </xs:sequence>
                        <xs:attribute name="Version" type="xs:integer" />
                    </xs:complexType>
                </xs:element>
    - <xs:element name="NewConfig">
        - <xs:complexType>
```

```
            - <xs:sequence>
                <xs:element name="Command" maxOccurs="unbounded" />
              </xs:sequence>
                          <xs:attribute name="Vesrion" type="xs:integer" />
                      </xs:complexType>
                  </xs:element>
              </xs:sequence>
              <xs:attribute name="CASLogID" type="xs:integer" />
              <xs:attribute name="DeviceName" type="xs:string" />
          </xs:complexType>
      </xs:element>
</xs:schema>
```

Detailed Description of Configuration Management Schema

The table below describes elements in the Configuration Management schema.

Field	Description
Category	Type of the change. For example, configuration, inventory, or software.
Host	Host device from which the user accessed the device or the host name of the LMS server.
Application	Name of the application. For example, Archive Mgmt, NetConfig, etc.
User	Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the LMS is running, or the name under which the Telnet connection is established.
Device	Network device on which the change occurred. The display name as entered in the Device and Credential Repository.
ConnectionMode	Connection mode through which the change was made, for example, Telnet, snmp, console, or LMS.
Timestamp	Date and time at which the application communicated the network change or when Change Audit saw the change record.
Summary	Description describing what caused the change. For example: • Configuration Download due to job • Syslog triggered Config Collection
ConfigDiff	• FirstConfig, SecondConfig • DeviceName—Network device on which the change occurred. The display name as entered in the Device and Credential Repository. • Version—Configuration file version number. • CommandDiff Polarity—Changes in the configuration file. – POSNEG—No change – POSITIVE —Added new commands – IGNORED—Ignored the commands – NEGATIVE—Deleted the commands

XML Schema for Inventory Collection Service

The following XML schema is used by Inventory Collection Service application when you run the **cwcli export changeaudit** command with **-app** argument and the **-app** argument values as ICServer.

The schema file is:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<xsd:schema xmlns:xsd = "http://www.w3.org/2000/10/XMLSchema">
<xsd:element name = "InventoryChangeDetailRecord">
    <xsd:complexType>
        <xsd:sequence maxOccurs = "unbounded">
            <xsd:element ref = "Section"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name = "Section">
    <xsd:complexType>
        <xsd:sequence maxOccurs = "unbounded">
            <xsd:element ref = "Attributes"/>
        </xsd:sequence>
        <xsd:attribute name = "Name" type = "xsd:string"/>
        <xsd:attribute name = "Identity" type = "xsd:string"/>
    </xsd:complexType>
</xsd:element>
<xsd:element name = "Attributes">
    <xsd:complexType>
        <xsd:all maxOccurs = "unbounded">
            <xsd:element ref = "Previous_value"/>
            <xsd:element ref = "Current_value"/>
            <xsd:element ref = "Action"/>
        </xsd:all>
    </xsd:complexType>
</xsd:element>
    <xsd:element name = "Previous_value" type = "xsd:string"/>
    <xsd:element name = "Current_value" type = "xsd:string"/>
    <xsd:element name = "Action" type = "xsd:string"/>
</xsd:schema>
```

Detailed Description of Inventory Collection Service Schema

The table below describes elements in the Inventory Collection Service schema.

Field	Description
Name	Name of the physical and logical entities. The main physical entities are Chassis, Backplane, Card, CommunicationConnector, FlashDevice, FlashPartition, FlashFile, SoftwareIdentity, PhysicalMemory The main logical entities are ManagedNetworkElement, LogicalModule, Port, MemoryPool, OSElement, IPProtocolEndpoint, IfEntry, AdditionalInformation See Detailed Description of the Inventory Schema for further information.
Identity	Identifies the entity that has changed on the device. For example: If the Flash File name has changed then Identity will be Flash Device 2, Flash Partition 3.

Field	Description
AttributeName	Name of the different physical and logical entities For example: In MemoryPool, the different entities are User, Free, PoolType. See Detailed Description of the Inventory Schema for further information.
Previous_value	Value of the entity before the change occurred.
Current_value	Value of the entity after the change occurred.
Action	Type of change that has occurred on the device: • Inserted— Added a new entity. • Changed—Changed in the entity. • Deleted—Deleted an entity.

XML Schema for Software Management

The following XML schema is used by Software Management application when you run the **cwcli export changeaudit** command with **-app** argument and the **-app** argument values as Software Management.

The schema file is:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--  edited with XMLSPY v2004 rel. 2 U (http://www.xmlspy.com) by Cisco -->
- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
- <xs:element name="SwimHistoryRecord">
    - <xs:annotation>
        <xs:documentation>Models a set of image changes on the device.</xs:documentation>
    </xs:annotation>
- <xs:complexType>
    - <xs:sequence>
        - <xs:element name="JobID" type="xs:positiveInteger" minOccurs="0">
    - <xs:annotation>
        <xs:documentation>ID of the Job in which the change happened</xs:documentation>
    </xs:annotation>
    </xs:element>
    - <xs:element name="ImageChange" maxOccurs="unbounded">
- <xs:complexType>
    - <xs:sequence>
          <xs:element name="OldImage" type="Image" />
          <xs:element name="NewImage" type="Image" />
      </xs:sequence>
      <xs:attribute name="ID" type="xs:positiveInteger" use="required" />
      </xs:complexType>
      </xs:element>
      </xs:sequence>
  </xs:complexType>
</xs:element>
- <xs:complexType name="Image">
- <xs:annotation>
     <xs:documentation>Models an Image.</xs:documentation>
  </xs:annotation>
- <xs:sequence>
    - <xs:element name="Type">
        - <xs:annotation>
          <xs:documentation>Label of corresponding image type from enumeration
        com.cisco.nm.xms.xdi.ags.imageparser.ImageType</xs:documentation>
          </xs:annotation>
```

```
        - <xs:simpleType>
            - <xs:restriction base="xs:string">
            <xs:whiteSpace value="preserve" />
          </xs:restriction>
        </xs:simpleType>
        </xs:element>
      <xs:element name="Name" type="xs:string" />
      <xs:element name="Version" type="xs:string" />
- <xs:element name="Attribute" minOccurs="0" maxOccurs="unbounded">
    - <xs:complexType>
    - <xs:sequence>
        - <xs:element name="AttributeName">
        - <xs:simpleType>
            - <xs:restriction base="xs:string">
            <xs:whiteSpace value="preserve" />
      </xs:restriction>
      </xs:simpleType>
  </xs:element>
- <xs:element name="AttributeValue">
    - <xs:simpleType>
        - <xs:restriction base="xs:string">
         <xs:whiteSpace value="preserve" />
      </xs:restriction>
      </xs:simpleType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:schema>
```

Detailed Description of Software Management Schema

The table below describes elements in the Software Management schema.

Field	Description
Category	Type of the change. For example, configuration, inventory, or software.
Host	Host device from which the user accessed the device or the host name of the LMS server.
Application	Name of the application. For example, Archive Mgmt, NetConfig, etc.
User	Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the LMS is running, or the name under which the Telnet connection is established.
Device	Network device on which the change occurred. The display name as entered in the Device and Credential Repository.
ConnectionMode	Connection mode through which the change was made, for example, Telnet, snmp, console, or LMS.
Timestamp	Date and time at which the application communicated the network change or when Change Audit saw the change record.
Summary	Description describing what caused the change. For example, Software upgrade.
Job ID	Job ID for the Software Upgrade.

Field	Description
OldImage	Displays the details on device type, name of the software image, and version of the image.
NewImage	Displays the details on device type, name of the software image, and version of the image.

Usage Examples for cwcli export changeaudit Command

This section provides some examples of usage for the **cwcli export changeaudit** command.

Example 1: To generate the Change Audit report for all applications and categories for a particular device group.

cwcli export changeaudit -u *admin* **-p** *admin* **-view** *"/RME@ciscoworksservername/Normal Devices*"

```
SUMMARY
========
        Successful: export:
D:/PROGRA~1/CSCOpx/files/rme/archive/2004-10-15-04-09-42-changeaudit.xml
```

Example 2: To generate the Change Audit report for a specific application and category for a device in a given time frame

cwcli export changeaudit -u *admin* **-p** *admin* **-device** *10.6.8.6* **-from** *09/30/2004* **-to** *10/15/2004* **-app** "*Archive Mgmt*" **-cat** *CONFIG_CHANGE*

```
SUMMARY
========
        Successful: export:
D:/PROGRA~1/CSCOpx/files/rme/archive/2004-10-15-04-44-50-changeaudit.xml
```

Example 3: To generate the Change Audit report in the given output file

cwcli export changeaudit -u *admin* **-p** *admin* **-device** *%* **-f** *changeaudit.xml*

```
SUMMARY
========
        Successful: export: changeaudit.xml
```

The output for this is written to the changeaudit.xml file in the *Install_dir*/CSCOpx/bin directory. Where *Install_dir* is the LMS installed directory.

Example 4: To generate the Change Audit using the cwcli get request

The password that you enter here must be in base64 encoded.

In this example,

- *YWRtaW4=* is the base64 encoded password for admin.
- %25 is the URL encode for “%”
- %2f is the URL encode for “_”

Enter this in your browser:

http://*ciscowork_servername*:1741/rme/cwcli?command=cwcli export changeaudit -u *admin* -p *YWRtaW4=* -device *10.7.3.8* -app *%22Archive Mgmt%22* -cat *%22CONFIG%2fCHANGE%22* -f *changeaudit.xml*

The output for this is written to the changeaudit.xml file.The changeaudit.xml file is located:

On Windows:

NMSROOT\MDC\tomcat

Where, *NMSROOT* is the LMS installed directory.

On Solaris and Soft Appliance:

NMSROOT/objects/dmgt

Example 5: To generate the Change Audit report using cwcli post request method

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

The payload file, *changeaudit.xml* contains:

```
<payload>
   <command>
cwcli export changeaudit -u admin -p YWRtaW4= -device 1.6.8.6 -from 09/30/2004 -app
"Archive Mgmt" -cat CONFIG_CHANGE -view "/RME@CiscoWorks_servername/Pre-deployed" -f
changeauditreport.xml
   </command>
</payload>
```

At the command prompt enter:

perl *samplepost.pl* **https://LMS_Servername:443/rme/cwcli** *changeaudit.xml*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
SUMMARY
========
        Successful: export: changeauditreport.xml
<!-- Processing complete -->
```

The output for this is written to the *changeauditreport.xml* file.The *changeauditreport.xml* file is located:

On Windows:

NMSROOT\MDC\tomcat

Where, *NMSROOT* is the LMS installed directory.

On Solaris and Soft Appliance:

NMSROOT/objects/dmgt

Running cwcli export config

Using this command you can retrieve the configuration data in the XML format specified by the schema. The Configlet Generator provides a wrapper over the existing Config Archive to retrieve configlets data for the selected device. The exported data contains the entire running configuration data.

The command syntax for **cwcli export config** is:

cwcli export config{**-u** *username* **-p** *password*} [**-d** *debuglevel*] [**-m** *mailid*] [**-l** *logfile*] {**-device** *devicename* | **-input** *inputfilename* | **-view** *viewname* | **- ipaddress** *mgmt-ip-address*}

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you enter an argument which has space then use double quotes for that argument.

The following table describes the argument that is specific to **cwcli export config** command. The other common arguments used by **cwcli export** are explained in Using the cwcli export Command.

Arguments	Description
-s 1	Optional. Displays the exported configuration file on the console. If you use this command, you can specify only one device. You cannot export the configuration files of multiple devices. To export the configuration files of multiple devices, either make multiple requests to the servlet, or get these files from the LMS server. Usage of this option: **cwcli export config -u** *admin* **-p** *admin* **-device** 10.22.33.44 **-s 1**

The output files depends on the number of devices specified. There are as many configuration XML output files as the number of devices. The output files are created under this location on LMS server:

On Solaris and Soft Appliance:
/var/adm/CSCOpx/files/rme/cwconfig/*YYYY-MM-DD-HH-MM-SS-XXX-Device_Display_Name.xml*

On Windows:
NMSROOT\files\rme\cwconfig*YYYY-MM-DD-HH-MM-SS-XXX-Device_Display_Name.xml*

Where *NMSROOT* is the LMS installed directory.

XML Schema for cwcli export config

The following is the schema used for exporting the configuration data in XML format.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSPY v5 rel. 4 U (http://www.xmlspy.com) by Cisco -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xs:element name="DeviceConfiguration">
<xs:annotation>
<xs:documentation>This has list of Configlets</xs:documentation>
</xs:annotation>
<xs:complexType>
<xs:sequence>
<xs:element ref="Confilglet" maxOccurs="unbounded"/>
<xs:element name="DeviceName" type="xs:string">
<xs:annotation>
<xs:documentation>Device Name as managed by RME</xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="DeviceFamily" type="xs:string">
<xs:annotation>
<xs:documentation>MDF devcie family</xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="CreationTime" type="xs:date">
<xs:annotation>
<xs:documentation>Date and Time this was created</xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="Version" type="xs:string">
<xs:annotation>
<xs:documentation>Config File Version</xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="Data" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Confilglet">
<xs:annotation>
<xs:documentation>Configlet can have subconfiglets</xs:documentation>
</xs:annotation>
<xs:complexType>
<xs:sequence>
<xs:element ref="Confilglet" minOccurs="0" maxOccurs="unbounded"/>
<xs:element name="command" minOccurs="0" maxOccurs="unbounded">
<xs:complexType>
<xs:simpleContent>
<xs:extension base="xs:string">
<xs:attribute name="LineNo"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name="SubModeCommand" type="xs:string" minOccurs="0">
<xs:annotation>
<xs:documentation>Command to change the mode</xs:documentation>
</xs:annotation>
</xs:element>
</xs:sequence>
<xs:attribute name="Name" type="xs:string" use="required">
<xs:annotation>
<xs:documentation>Configlet Name</xs:documentation>
```

```
</xs:annotation>
</xs:attribute>
<xs:attribute name="Checkedout" type="xs:boolean" use="optional" default="false">
<xs:annotation>
<xs:documentation>Future Use </xs:documentation>
</xs:annotation>
</xs:attribute>
<xs:attribute name="Rebuild" type="xs:boolean" use="optional" default="false">
<xs:annotation>
<xs:documentation>Specifies if the entire list of commands in particular configlet needs a rebuild if any of
the coammnds is modified</xs:documentation>
</xs:annotation>
</xs:attribute>
<xs:attribute name="Submode" type="xs:boolean" use="optional" default="false">
<xs:annotation>
<xs:documentation>Specfies if the commands under the configlet falls under a submode</xs:documentation>
</xs:annotation>
</xs:attribute>
<xs:attribute name="OrderSensitive" type="xs:boolean" use="optional" default="false">
<xs:annotation>
<xs:documentation>Specifies if the commands in the configlet are oreder sensitive or not</xs:documentation>
</xs:annotation>
</xs:attribute>
</xs:complexType>
</xs:element>
</xs:schema>
```

Detailed Description of config Schema

The table below describes elements in the config schema:

Field	Description
Device	Device display name as entered in the Device and Credential Repository.
Date	Date and time at which the configuration changes have occurred.
Version	Configuration file version.
Configlet name	Name of the configlet. The available configlets vary from device to device; the following are examples: • SNMP displays SNMP configuration commands, for example, snmp-server community public RO. • IP Routing displays IP routing configuration commands, for example, router abcd 100. • Interface folder displays the different interface configuration commands, for example, Interface Ethernet0 and Interface TokenRing. • Global displays global configuration commands, for example no ip address. • Line con 0 displays configuration commands for line console 0. • IP displays IP configuration commands, for example, **`ip http server`**.

Usage Examples for cwcli export config Command

This section provides some examples of usage for the **cwcli export config** command.

Example 1: To generate the config report for a particular device group

cwcli export config -u *admin* **-p** *admin* **-view** *"/RME@ciscoworksservername/Normal Devices*"

```
SUMMARY
========
        Successful: ConfigExport:D:/PROGRA~1/CSCOpx/files/rme/cwconfig
```

The output folder will contain separate config file for every devices in the Normal Devices group.

Example 2: To generate the config report for the devices that are specified in the device input file

The input configdevices.txt contains these devices:

-device 10.22.33.44,10.22.33.55,1.1.1.1

cwcli export config -u *admin* **-p** *admin* **-input** *configdevices.txt*

Example 3: To generate the config using the cwcli get request

The password that you enter here must be in base64 encoded.

In this example,

- *YWRtaW4=* is the base64 encoded password for admin.
- %25 is the URL encode for "%"

Enter this in your browser:

http://*ciscowork_servername***:1741/rme/cwcli?command=cwcli export config -u** *admin* **-p** *YWRtaW4=* **-device** *%25*

```
<!-- Processing Starts  -->
SUMMARY
========
Successful: ConfigExport: D:/PROGRA~1/CSCOpx/files/rme/cwconfig
<!-- Processing complete -->
```

Example 4: To generate the Change Audit report using cwcli post request method

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

The payload file, *config.xml* contains:

```
<payload>
   <command>
cwcli export config -u admin -p YWRtaW4= -device 1.6.8.6
   </command>
</payload>
```

At the command prompt enter:

perl *samplepost.pl* **https://LMS_Servername:443/rme/cwcli** *config.xml*

```
<!-- Processing Starts  -->
```

```
SUMMARY
========
        Successful: ConfigExport: D:/PROGRA~1/CSCOpx/files/rme/cwconfig
<!-- Processing complete -->
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

Running cwcli export inventory Command

Using this command you can export inventory data in the XML format.

The command syntax for **cwcli export inventory** is:

cwcli export inventory {**-u** *username* **-p** *password*}[**-d** *debuglevel*] [**-m** *mailid*] [-l *logfile*] [**-f** *filename*] {**-device** *devicename* | **-input** *inputfilename* | **-view** *viewname* | **- ipaddress** *mgmt-ip-address*} [**-hop** *hopdevice*]

The above command retrieves the inventory data in XML format specified by the schema. The **-f** parameter stores the output in the file specified by *filename*. If you have not specified the filename, the output is stored at the following location:

PX_DATADIR/rme/archive/timestampinventory.xml (On Solaris and Soft Appliance)

PX_DATADIR\rme\archive\timestampinventory.xml (On Windows)

Where *PX_DATADIR* is the *NMSROOT*/files directory and *NMSROOT* is the LMS installed directory.

The device name can also have a wild card symbol "**%**" to choose all devices with that particular name.

If the number of devices is large, the list of devices can be stored in an input file and the name of the input file can be given in the command line.The input argument cannot occur with the device or view arguments.

If the data needs to be generated for all the devices in a specific group, you can use the **-view** argument. You can use this argument to generate data for devices in all device groups including system-defined groups and user-defined groups.

The following table describes the arguments that are specific to **cwcli export inventory** command. The other common arguments used by **cwcli export** are explained in Using the cwcli export Command.

Global Arguments	Description
-hop *hopdevice*	Optional Used to increase performance by using more memory. This indicates the number of devices to be worked upon at a time. By default, this value is 1.

Given below is the list of combinations, which could occur for the inventory command.

cwcli export inventory -u *admin* **-p** *admin* **-f** *myinv.xml*

cwcli export inventory -u *admin* **-p** *admin* **-f** *myinv.xml* **-device** *device1*

cwcli export inventory -u *admin* **-p** *admin* **-device** *device%*

cwcli export inventory -u *admin* **-p** *admin* **-input** *inv.txt*

cwcli export inventory -u *admin* **-p** *admin* **-view** *"/RME@ciscoworksservername/Normal Devices*"

cwcli export inventory -u *admin* **-p** *admin* **-f** *myinv.xml* **-input** *inv.txt*

To apply the **cwcli export** command on more than one LMS device you must use the format in the example given below. The parameter, inputlist, is a text file which will have the list of device names separated by a new line. A line starting with # will be treated as a comment.

Example:

```
#comment
-device device1,device2,device3
#comment
```

where device1, device2, and device3 are device displaynames.

XML Schema for cwcli export inventory Data

The following is the schema used for exporting the inventory data in XML format.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<xs:schema xmlns:xs = "http://www.w3.org/2001/XMLSchema" elementFormDefault = "qualified"
attributeFormDefault = "unqualified">
        <!--This schema is based on the classes defined in Cisco Information Model V2.0 (CIMCXV2.0)
Each Device has Chassis and NetworkElement.
Chassis:
        Chassis contains a blackplane and multiple Cards. Each Card contains CommunicationConnectors and
multiple daughter cards. Flash Devices reside on the Cards.
NetworkElement:
System Information, Interface Information and LogicalModules. LogicalModules contain OSElements and Logical
Ports.
The element AdditionalInformation is meant to capture device specific details that are not part of the common
schema.
-->
<xs:element name = "InvDetails">
<xs:complexType>
<xs:sequence>
<xs:element ref = "SchemaInfo" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "RMEPlatform" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "SchemaInfo">
<xs:complexType>
<xs:sequence>
<xs:element name = "RMEServer" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "CreatedAt" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SchemaVersion" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "RMEPlatform">
<xs:complexType>
<xs:sequence>
<xs:element ref = "Cisco_Chassis" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_NetworkElement" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_ComputerSystemPackage" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref= "Cisco_EnergyWise" minOccurs="0" maxOccurs= "1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_Chassis">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
```

```
<xs:element name = "Model" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "HardwareVersion" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SerialNumber" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ChassisSystemType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfSlots" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NoOfCommunicationConnectors" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_Backplane" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_Card" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_Backplane">
<xs:complexType>
<xs:sequence>
<xs:element name = "BackplaneType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Model" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SerialNumber" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_Card">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "RequiresDaughterBoard" type = "xs:boolean" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Model" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SerialNumber" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "LocationWithinContainer" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PartNumber" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "CardType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "HardwareVersion" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "OperationalStatus" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FWManufacturer" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Manufacturer" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfSlots" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NoOfCommunicationConnectors" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "SoftwareIdentity" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_CommunicationConnector" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_FlashDevice" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_PhysicalMemory" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_Card" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_CommunicationConnector">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ConnectorType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "POEAdminStatus" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "MaximumPower" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PowerAllocated" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_FlashDevice">
<xs:complexType>
<xs:sequence>
```

```
<xs:element name = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FlashDeviceType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Size" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfPartitions" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ChipCount" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Removable" type = "xs:boolean" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_FlashPartition" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_FlashPartition">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Upgrade" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NeedsErasure" type = "xs:boolean" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PartitionStatus" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "unknown"/>
<xs:enumeration value = "readOnly"/>
<xs:enumeration value = "runFromFlash"/>
<xs:enumeration value = "readWrite"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "FileSystemSize" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "AvailableSpace" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FileCount" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_FlashFile" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_FlashFile">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FileSize" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FileStatus" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "unknown"/>
<xs:enumeration value = "deleted"/>
<xs:enumeration value = "invalidChecksum"/>
<xs:enumeration value = "valid"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "Checksum" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_PhysicalMemory">
<xs:complexType>
<xs:sequence>
<xs:element name = "MemoryType" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
```

```
<xs:restriction base = "xs:string">
<xs:enumeration value = "nvRam"/>
<xs:enumeration value = "NVRAM"/>
<xs:enumeration value = "processorRam"/>
<xs:enumeration value = "RAM"/>
<xs:enumeration value = "ROM"/>
<xs:enumeration value = "FEPROM"/>
<xs:enumeration value = "BRAM"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "Capacity" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_NetworkElement">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:integer" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PrimaryOwnerName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PhysicalPosition" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SysObjectId" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SysUpTime" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "OfficialHostName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfPorts" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_LogicalModule" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_Port" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_MemoryPool" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_IfEntry" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_IPProtocolEndpoint" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_PEHasIfEntry" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_LogicalModule">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ModuleNumber" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ModuleType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "EnabledStatus" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfPorts" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_Port" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_LogicalModule" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_OSElement" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_Port">
<xs:complexType>
<xs:sequence>
<xs:element name = "PortNumber" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PortType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "IfInstanceID" type = "xs:integer" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
```

```
</xs:element>
<xs:element name = "Cisco_MemoryPool">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PoolType" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "DynamicPoolType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "AlternatePoolType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "IsValid" type = "xs:boolean" minOcurs = "0" maxOccurs = "1"/>
<xs:element name = "Allocated" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Free" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "LargestFree" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
<!--PoolType ValueMap  {"0", "1", "2", "3", "4", "5", "65536"},
Values {"Unknown", "Processor", "I/O", "PCI", "Fast", "Multibus", "Dynamic"},
-->
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_OSElement">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "OSFamily" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Version" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_IfEntry">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ProtocolType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Speed" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "RequestedStatus" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "up"/>
<xs:enumeration value = "down"/>
<xs:enumeration value = "testing"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "OperationalStatus" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "Up"/>
<xs:enumeration value = "Down"/>
<xs:enumeration value = "Testing"/>
<xs:enumeration value = "Unknown"/>
<xs:enumeration value = "Dormant"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PhysicalAddress" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NetworkAddress" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
```

```
<xs:element name = "Cisco_IPProtocolEndpoint">
<xs:complexType>
<xs:sequence>
<xs:element name = "Address" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SubnetMask" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "DefaultGateway" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_PEHasIfEntry">
<xs:complexType>
<xs:sequence>
<xs:element name = "Cisco_IPProtocolEndpoint" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Cisco_IfEntry" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_ComputerSystemPackage">
<xs:complexType>
<xs:sequence>
<xs:element name = "Antecedent" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Dependent" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<!--
Antecedent is the InstanceID from Cisco_Chassis Element
Dependent is the InstanceID from Cisco_NetworkElement
-->
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Cisco_EnergyWise">
<xs:complexType>
<xs:sequence>
<xs:element name= "InstanceID" type= "xs:string" minOccurs= "0" maxOccurs= "1"/>
<xs:element name= "DomainName" type= "xs:string" minOccurs= "0" maxOccurs= "1"/>
<xs:element name= "Role" type= "xs:string" minOccurs= "0" maxOccurs="1"/>
<xs:element name= "Keyword" type= "xs:string" minOccurs= "0" maxOccurs= "1"/>
<xs:element name= "Importance" type= "xs:string" minOccurs= "0" maxOccurs= "1"/>
<xs:element ref= "Cisco_EnergyWiseInterface" minOccurs= "0" maxOccurs= "1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name= "Cisco_EnergyWiseInterface">
<xs:complexType>
<xs:sequence>
<xs:element name= "InstanceID" type= "xs:string" minOccurs= "0" maxOccurs= "1"/>
<xs:element name= "Description" type= "xs:string" minOccurs= "0" maxOccurs= "1"/>
<xs:element name= "Role" type= "xs:string" minOccurs= "0" maxOccurs= "1"/>
<xs:element name= "Keyword" type= "xs:string" minOccurs= "0" maxOccurs= "1"/>
<xs:element name= "Importance" type= "xs:string" minOccurs= "0" maxOccurs= "1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "SoftwareIdentity">
<xs:complexType>
<xs:sequence>
<xs:element name = "Classification" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "Firmware"/>
<xs:enumeration value = "Software"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
```

```
<xs:element name = "VersionString" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "AdditionalInformation">
<xs:complexType>
<xs:sequence>
<xs:element name = "AD" minOccurs = "0" maxOccurs = "unbounded">
<xs:complexType>
<xs:attribute name = "name" type = "xs:string"/>
<xs:attribute name = "value" type = "xs:string"/>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

Detailed Description of the Inventory Schema

The inventory schema provides the structure for the inventory information exported from LMS. The schema divides inventory information into two groups:

- Physical Inventory
- Logical Inventory

The Physical Inventory contains the chassis information and related details for the device. The main elements in the schema for the physical inventory part are:

- Chassis (Cisco_Chassis
- Backplane (Cisco_ Backplane
- Card (Cisco_Card)
- CommunicationConnector (Cisco_CommunicationConnector)
- FlashDevice (Cisco_FlashDevice)
- FlashPartition (Cisco_FlashPartition)
- FlashFile (Cisco_FlashFile)
- .SoftwareIdentity (Cisco_SoftwareIdentity)
- PhysicalMemory (Cisco_PhysicalMemory)

The Logical Inventory part of the schema contains the details of the managed network element. The main elements in the schema for the logical inventory part are:

- .ManagedNetworkElement (Cisco_NetworkElement)
- LogicalModule (Cisco_LogicalModule)
- Port (Cisco_Port)
- MemoryPool (Cisco_MemoryPool)
- OSElement (Cisco_OSElement)
- IPProtocolEndpoint (Cisco_IPProtocolEndpoint)
- IfEntry (Cisco_IfEntry)
- Additional Information

Chassis (Cisco_Chassis

The Chassis class represents the physical elements that enclose other elements in the device and provide specific functions, such as a desktop, networking node, UPS, disk or tape storage, or a combination of these functions.

The following table describes the elements in Chassis:

Element	Description
InstanceID	Unique identifier.
Model	Chassis model / Chassis ID.
Version	Hardware version of the chassis
SerialNumber	Serial number associated with the chassis.
Type	Chassis type.

Element	Description
NumberOfSlots	Number of slots in a chassis.
NoOfCommunicationConnectors	Number of physical connectors in a chassis.

Chassis also contains the elements Card and Backplane.

Backplane (Cisco_ Backplane

Backplane is an instance of a backplane in a chassis. The following table describes the elements in Backplane:

Element	Description
BackplaneType	Type of backplane
Model	Model of the backplane
SerialNumber	Serial number of the backplane.

Card (Cisco_Card)

Card represents:

- A type of physical container that can be plugged into another card, motherboard, or hosting board
- A motherboard or hosting board in a chassis

This element includes any package capable of carrying signals and providing a mounting point for physical components such as chips, or other physical packages such as other cards. The following table describes the elements in Card:

Element	Description
InstanceID	Card number. This is used to correlate with the logical part of the card.
Model	Model of the card.
SerialNumber	Serial number of the card.
LocationWithinContainer	Number that indicates the physical slot number. This can be used as an index into a system slot table, irrespective of whether that slot is physically occupied or not.
PartNumber	Part number of the Hardware Component.
CardType	Type of the card (Card Type)
Description	Descriptive string used to describe the card.
OperationalStatus	Status of the card describing whether it is up or down
FWManufacturer	Manufacturer of the firmware
Manufacturer	Manufacturer of the hardware
NumberOfSlots	Number of slots in the card.
NoOfCommunicationConnectors	Number of ports in the card.

Apart from the elements described in the table above, the card element also contains reference to itself, which can represents a sub card. It also contains other elements such as CommunicationConnector and FlashDevice.

CommunicationConnector (Cisco_CommunicationConnector)

CommunicationConnector represents a physical port. The table below describes the elements in CommunicationConnector:

Element	Description
InstanceID	Indicates the connector number for the chassis or system.
ConnectorType	Type of the physical port.
Description	Descriptive string used to describe the card.

FlashDevice (Cisco_FlashDevice)

FlashDevice represents physical flash memory. Flash memory may reside on a PCMCIA card, line card, or any other type of card. FlashDevice may consist of one or more actual flash memory chips.

It also consists of reference to one or more flash partitions described in FlashPartition. The table below describes the elements in FlashDevice.

Element	Description
InstanceID	FlashDevice sequence number to index the flash devices within the table of initialized FlashDevices.
InstanceName	Name of FlashDevice. This name is used to refer to the device within the system. Flash operations get directed to a device based on this name.
Size	Total size of FlashDevice. For a removable device, the size will be zero if the device has been removed.
NumberOfPartitions	Number of Flash partitions present in f FlashDevice
ChipCount	Total number of chips within FlashDevice. This element provides information to a network management station on how much chip information to expect. It also helps the management station to check the chip index against an upper limit when randomly retrieving chip information for a partition.
Description	Description of a FlashDevice. The description is meant to explain what FlashDevice is and its purpose.
Removable	Specifies whether FlashDeviceis removable. Typically, only PCMCIA Flash cards are treated as removable. Socketed Flash chips and Flash SIMM modules are not treated as removable.

FlashPartition (Cisco_FlashPartition)

FlashPartition corresponds to the Cisco-flash-mib. The elements in FlashPartiion are derived from the table of properties of ciscoFlashPartitionTable for each initialized flash partition.

When there is no explicit partitioning for a device, it is assumed that there is a single partition spanning the entire device exists. Therefore, a device always has at least one partition.

FlashPartition contains one or more FlashFileSystems as described in FlashFile. The table below describes the elements in FlashPartition.

Element	Description
InstanceID	FlashPartition sequence number used to index FlashPartitions within the table for initialized FlashPartitions.
InstanceName	FlashPartition name used to refer to a partition by the system.
PartitionStatus	Status of the partition.
Upgrade	Upgrade information for the partition. This helps to download new files into the partition, and is needed when the PartitionStatus is run from flash.
NeedsErasure	Boolean parameter indicating whether the partition requires to be erased before any write operations can occur.
Size	FlashPartition size. It should be an integral multiple of ciscoFlashDeviceMinPartitionSize. If there is a single partition, this size will be equal to ciscoFlashDeviceSize.
FreeSpace	Free space within aFlashPartition.
FileCount	Number of files stored in the file system.

FlashFile (Cisco_FlashFile)

FlashFile manages the storage and organization of files on a Flash memory device. The table below describes the elements in FlashFile

Element	Description
InstanceID	FlashFile sequence number used to index within a FlashPartition directory table.
FileSize	Size of the file in bytes.This size does not include the size of the filesystem file header.
FileStatus	Status of a file. A file could be explicitly deleted if the file system supports such a user command. Alternatively, an existing good file would be automatically deleted if another good file with the same name were copied in. Deleted files continue to occupy prime space in flash memory. A file is marked as having an invalid checksum if any checksum mismatch was detected while writing or reading the file. Incomplete files (files truncated either because of lack of free space, or because of a network download failure) are also written with a bad checksum and marked as invalid.
Checksum	File checksum stored in the file header. This checksum is computed and stored when the file is written into Flash memory, and serves to validate the data written into Flash. Where the system generates and stores the checksum internally in hexadecimal form, checksum provides the checksum in a string form. Checksum is available for all valid and invalid-checksum files.
FileName	FlashFile name as specified by the user while copying the file to Flash memory. The name should not include the colon (:) character as it is a special separator character used to separate the device name, partition name, and the file name.

.SoftwareIdentity (Cisco_SoftwareIdentity)

SoftwareIdentity provides the hardware and firmware version of the card. The table below describes elements in SoftwareIdentity.

Element	Description
Classification	Specifies whether the information is for hardware or firmware.
VersionString	Version information for software or firmware.

PhysicalMemory (Cisco_PhysicalMemory)

PhysicalMemory specifies the memory type and capacity of the device. The table below describes elements in PhysicalMemory.

Element	Description
MemoryType	Specifies the type of memory, that is whether RAM, ROM, or NVRAM.
Capacity	Capacity in bytes.

.ManagedNetworkElement (Cisco_NetworkElement)

ManagedNetworkElement is the entity that contains all logical parts of the device, which the users can configure (such as Logical Module, Port, Interfaces, Software Image details, and Memory Pool). The table below describes elements in ManagedNetworkElement.

Element	Description
InstanceID	Index number assigned to the network element.
Description	Description of the network element. This description includes the full name and version identification of the system's hardware type, operating system, and networking software. The description can have only printable ASCII characters.
PrimaryOwnerName	Identification of the contact person for this managed node, and information on how to contact this person.
InstanceName	Administratively defined name for the network element.
PhysicalPosition	Physical location of the network element.
SysObjectId	Vendor's authoritative identification of the management subsystem contained in the element.
SysUpTime	Time in hundredths of a second since the network management portion of the element was last initialized.
OfficialHostName	Name of the device.
NumberOfPorts	Number of ports in the network element.

LogicalModule (Cisco_LogicalModule)

LogicalModule is the logical device corresponding to a line card in the network device.

For example, a line card in a switch is an instance of LogicalModule, associated with the ManagedNetworkElement, in this case the switch. LogicalModule is not necessarily independently managed.

To represent a sub module, LogicalModule contains a reference to itself. It also contains Port and the OSElement. The table below describes the other elements in LogicalModule.

Element	Description
InstanceID	Index that correlates the physical card and the logical module. This helps to correlate the physical card to logical card details.
ModuleNumber	Number assigned to the module by its parent ManagedNetworkElement.
ModuleType	Type or model of the module.
InstanceName	Name of the logical module.
EnabledStatus	Status of the module, that is whether it is up or down.
NumberOfPorts	Number of ports in the logical module.

Port (Cisco_Port)

Port is the logical representation of network communications hardware - a physical connector and the setup or operation of the network chips, at the lowest layers of a network stack

For example, an Ethernet port on an Ethernet line card uses an instance of Port to represent its operational and logical properties. A port should be associated with either a LogicalModule or directly with a ManagedNetworkElement.

It also contains the element IPProtocolEndpoint. The table below describes the other elements in Port.

Element	Description
PortNumber	Number assigned to the port. Ports are often numbered relative to either a logical module or a network element.
PortType	Type of the port.
InstanceName	Name assigned to the port.
IfInstanceID	Index of the interface related to this port.

MemoryPool (Cisco_MemoryPool)

MemoryPool corresponds to entries to monitor entries. Each pool is a range of memory segregated by type or function. The table below describes the other elements in MemoryPool.

Element	Description
InstanceName	Name assigned to the MemoryPool.
PoolType	Dynamic type value assigned to a dynamic MemoryPool. This is valid only when the PoolType attribute has the value *Dynamic*. MemoryPools can be divided into two groups Predefined Pools and Dynamic Pools. For dynamic pools, the PoolType is set to the dynamic value (65536) and the DynamicPoolType is set to an integer value used to distinguish the various dynamic pool types.
DynamicPoolType	This attribute holds the dynamic type value assigned to a dynamic memory pool. It is only valid when the PoolType attribute has the value Dynamic (65536).
AlternatePoolType	Indicates whether this MemoryPool has an alternate pool configured. Alternate pools are used for fallback when the current pool runs out of memory. If the value is set to zero, then this pool does not have an alternate. Otherwise the value is the same as the value of PoolType of the alternate pool.
IsValid	Indicates whether the other attributes in this MemoryPool contain accurate data. If an instance of this object has the value, False, (indicating an internal error condition), the values of the remaining objects in the instance may contain inaccurate information. That is, the reported values may be less than the actual values.
Used	Indicates the number of bytes from the MemoryPool that are currently in use by applications on the managed device.
Allocated	Indicates the number of bytes from the MemoryPool that are currently unused on the managed device.
Free	Indicates the largest number of contiguous bytes from the MemoryPool that are currently unused on the managed device.

OSElement (Cisco_OSElement)

OSElement represents the software element that is deployed to a network system and describes the software behind the operating system.The table below describes the other elements in OSElement.

Element	Description
InstanceName	Name of the OS image.
Family	Family of the OS component.
Version	Version of the OS.
Description	Description of the OS image.

IPProtocolEndpoint (Cisco_IPProtocolEndpoint)

IPProtocolEndpoint contains the subnet mask and default gateway information corresponding to the management IP Address.

Element	Description
Address	IP address of this endpoint, formatted according to the convention as defined in the AddressType property of this class.
SubnetMask	Mask for the IP address of this element, formatted according to the convention as defined in the AddressType property of this class (e.g., 255.255.252.0).
DefaultGateway	Default gateway address.

IfEntry (Cisco_IfEntry)

IfEntry represents the contents of an entry in the ifTable as defined in RFC 1213.

Element	Description
InstanceID	Index in the interface table defined in RFC 1213 for the entry containing the interface attributes of this object.
InstanceName	ifName attribute in the interface table defined in RFC 1213.
IfType	Interface type enumeration taken from the IANA definition of ifType.
IfSpeed	Estimate of the current bandwidth of the interface in bits per second. In cases, where the current bandwidth cannot be given, the nominal bandwidth should be specified.
IfAdminStatus	Desired state of the interface.
IfOperStatus	Current operational status of the interface.
Description	Description of the interface.
PhysicalAddress	Hardware address of the interface.
NetworkAddress	Network address of the interface.

Additional Information

AdditionalInformation is used to describe device specific information. It contains name and value attributes for elements specific to the device.

Class	Element	AdditionalInformation Tag
Cisco Call Manager	Cisco_NetworkElement	ActivePhones, InActivePhones, ActiveGateways, InActiveGateways, CallManagerIndex, CallManagerName, CallManagerDescription, CallManagerVersion, CallManagerStatus
	Cisco_Chassis	ApplicationPackageIndex, PackageManufacturer, Productname, Packageversion, Package SerialNumber

Class	Element	AdditionalInformation Tag
Cisco FastSwitch With_Module	Cisco_NetworkElement	FwdEngRev, BoardRev, SwitchPortNumber , SharedPortNumber, FirmwareSource
	Cisco_FlashDevice	FlashBankStatus
	Cisco_Card	InstanceID, ID
Cisco Firewall	None	None
Cisco IPX-IGX-BPX	Cisco_Chassis	InstanceName , Number
	Cisco_Card	SecondarySwRev, slotIndex, RAMId, ROMId, BRAMId, BOOTId, LocationWithinContainer, SecondaryStatus
	Cisco_Port	switchIfSlot,switchIfPort, SubPortNo, Status, Speed, PortType
Cisco LS1010 Switch	Cisco_Chassis	Slot0 (Type), Slot1(Type), AvailableSlots
	Cisco_NetworkElement	ConfigReg
	Cisco_PhysicalMemory	NVRAMUsed, RomVersion
Cisco MGX	Cisco_Chassis	Name, switchIfSlot, switchIfPort, SubPortNo, Status, Speed, PortType
Cisco Catalyst 3900 Switch	Cisco_Chassis	ModuleCount, Configuration, SwitchCount
	Cisco_Card	CiscoTsNumber, PermanentMAC, LocalMAC, CiscoTsModNumber , StackNo
Cisco Router 700 Series	Cisco_Chassis	MACAddress, PortCount, Type
Cisco Router	Cisco_PhysicalMemory	NVRAMUsed, ROMVersion
	Cisco_NetworkElement	Config
Cisco Catalyst IOS Switch	Cisco_Chassis	MACAddress, PortCount, Type
	Cisco_Card	FlashSize,FlashFree,FlashCard
	Cisco_Chassis	Config
	Cisco_PhysicalMemory	NVRAMUsed, ROMVersion
Cisco Catalyst L2L3 Switch	Cisco_Chassis	Slot0, Slot1 , MACAddress, PortCount, Type
	Cisco_NetworkElement	Config
	Cisco_PhysicalMemory	NVRAMUsed, ROMVersion
Cisco VPN 3000 Concentrators	Cisco_Chassis	PowerSupply1Type, PowerSuppy2Type, RAMSize
	Cisco_Card	LocationWithinContainer, CryptoHardwareType, SepState, DSPCodeVersion
Cisco Catalyst Switch	Cisco_Chassis	PowerSupply1, PowerSupply2 , MgmtType, BroadcastAddress, AvailableSlots
	Cisco_Card	ModuleIndex, RedundantModule, ModuleSubType
	Cisco_LogicalModule	moduleIndex,ModuleIPAddress
Cisco Optical Switches	Cisco_NetworkElement	RFUnitDetected, RFUnitID, RFUnitState, RFPeerUnitID, RFPeerUnitState, ActivateRF, ManualSwitchPermitted , StartupSyncStatus, RunningSyncStatus
	Cisco_PhysicalMemory	NVRAMUsed

Class	Element	AdditionalInformation Tag
Cisco FastSwitch	Cisco_NetworkElement	FwdEngRev, BoardRev, SwitchPortNumber , SharedPortNumber, FirmwareSource
	Cisco_FlashDevice	FlashBankStatus
	Cisco_Chassis	EPROMRev
	Cisco_CommunicationConnector	swPortIndex , PortTableSize, RevName, Type
Cisco Content Service Switch	None	None
Cisco Aironet	Cisco_PhysicalMemory	NVRAMUsed, ROMVersion
	Cisco_NetworkElement	Config
Cisco NAM	None	None
Cisco Management Engines	None	None

Overview: cwcli inventory Command

The **cwcli inventory** is a Device Management application command line tool. This tool supports the following features:

- You can check the specified device credentials for the devices.
- You can export device credentials of one or more devices in clear text.
- You can delete the specified devices.
- You can view the devices state.

The **cwcli inventory** command is located in the following directories, where *install_dir* is the directory in which LMS is installed:

- On Solaris and Soft Appliance systems, /opt/CSCOpx/bin
- On Windows systems, *install_dir*\CSCOpx\bin

  The default install directory is C:\Program Files.

This section contains:

- Using the cwcli inventory Command
- Running the cwcli inventory cda Command
- Running the cwcli inventory crmexport Command
- Running the cwcli inventory deletedevice Command
- Running the cwcli inventory getdevicestate Command

If you install LMS on an NTFS partition on Windows, only users in the administrator or casuser group can access **cwcli inventory**.

You can also perform the **cwcli inventory** tasks using the servlet. You will have to upload a payload XML file, which contains the **cwcli inventory** command arguments and LMS user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to run any command:

For post request,

perl *samplepost.pl* **http://***lms-server:lms-port***/rme/cwcli** *payload_XML_file*

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

perl *samplepost.pl* **https://***lms-server:lms-port***/rme/cwcli** *payload_XML_file*

The default port for LMS server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>
<command>
cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...
</command>
</payload>
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

For get request,

http://*lms-server:lms-port***/rme/cwcli?command=cwcli inventory** *commandname* **-u** *user* **-p** *BAse64 encoded pwd -args1 arg1value...*

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

https://*lms-server:lms-port***/rme/cwcli?command=cwcli inventory** *commandname* **-u** *user* **-p** *BAse64 encoded pwd -args1 arg1value...*

The default port for LMS server in HTTPS mode is 443.

The BAse64 encoded for “admin” is YWRtaW4=.

The URL encode for,

- Double quotes (“) is %22
- Percentage sign (%) is %25

Using the cwcli inventory Command

The command line syntax of the application is in the following format:

cwcli inventory *command GlobalArguments AppSpecificArguments*

The command line syntax of the application is in the following format:

cwcli export *command GlobalArguments AppSpecificArguments*

- **cwcli inventory** is the CiscoWorks command line interface for:
  - Checking the specified device credentials for the LMS devices.
  - Exporting device credentials of one or more LMS devices in clear text.
  - Deleting the specified LMS devices.

  - Viewing the LMS devices state.

- *Command* specifies which core operation is to be performed.
- *GlobalArguments* are the additional parameters required for each core command.
- *AppSpecificArguments* are the optional parameters, which modify the behavior of the specific `cwcli inventory` core command.

The order of the arguments and arguments are not important. However, you must enter the core command immediately after `cwcli inventory`.

The following sections describe:

- The `cwcli inventory` commands (See cwcli inventory Commands)
- The mandatory and optional arguments (See cwcli inventory Global Arguments)

On UNIX, you can view the `cwcli inventory` man pages by setting the MANPATH to /opt/CSCOpx/man. The man pages to launch the `cwcli inventory` are:

- man cwinventory-cda to launch the `cwcli inventory cda` command.
- man cwinventory-`delete` to launch the `cwcli inventory delete` command.
- man cwinventory-export to launch the `cwcli inventory export` command.
- man cwinventory-state to launch the `cwcli inventory getdevicestate` command

cwcli inventory Commands

The following table lists the command part of the `cwcli inventory` syntax:

Command	Description
`cwcli inventory cda`	You can check the specified device credentials for the devices. See Running the cwcli inventory cda Command
`cwcli inventory crmexport`	You can export device credentials of one or more devices in clear text. See Running the cwcli inventory crmexport Command
`cwcli inventory deletedevice`	You can delete the specified devices. See Running the cwcli inventory deletedevice Command
`cwcli inventory getdevicestate`	You can view the devices state. See Running the cwcli inventory getdevicestate Command

cwcli inventory Global Arguments

The following describes the mandatory and optional global arguments for `cwcli inventory`:

Argument	Description	Usage Notes
`-u` *user*	Enter a valid LMS username.	Mandatory.
`-p` *password*	Enter the password for the username.	Mandatory. You can provide this as part of argument or you can enter the password when you get the password prompt. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.
{`-device` *name* | `-view` *name* | `-device` *list* `-view` *name*| `-ipaddress` *list*}	`device` *name*—Enter the Display name of the device that you have added in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices)	Mandatory • You can enter multiple device list separated using a comma. For example, if there are two devices with Display Names Rtr12 and Rtr13, using Rtr% will display both the devices. • To include all the devices, use the wild card character "%". For example, To use all the devices, use `-device` %.
	`view` *name*—Enter the Device Group name.	Mandatory You can enter multiple group name separated using a comma. For view name, you have to enter the fully qualified path as in the Group Administration GUI. For example, `-view` "/RME@*ciscoworks_servername*/ All Devices"
	`device` *list* `view` *name*—Enter the Display name and the Device Group name.	Mandatory.
	`ipaddress` *list*—Enter the device IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated.	Mandatory. You cannot use this option with `-device`, `-view`, or `-input`. Also, you cannot specify wildcard characters.
[`-d` *debug_level*]	Enter the debug level.	Optional. *debug_level* is a number between 1 (the least information is sent to the debug output) and 5 (the most information is sent to the debug output). If you do not specify this argument, 4(INFO) is the default debug level.

Argument	Description	Usage Notes
[`-m` *email*]	Specify an e-mail address to send the results.	Optional. *email* is one or more e-mail addresses for notification. They can be separated by a space or comma.
[`-l` *logfile*]	Specify a file to which this command has to write log messages. The default log filename is cli.log. The default log directory is: On Windows: *NMSROOT*\log Where *NMSROOT* is the LMS installed directory. On Solaris and Soft Appliance: /var/adm/CSCOpx/log	Optional. Use the relative pathname to specify the *log_filename*.
`-help`	Displays command usage information	None.

Running the cwcli inventory cda Command

You can use this command to check the following device credentials:

- SNMP Read Community String—SNMP version 2 read community string.
- SNMP Write Community String—SNMP version 2 write community string.
- SNMP Version 3—SNMP version 3 username and password.
- Telnet—Telnet username and password.
- Telnet Enable Mode User Name and Password—Telnet username and password in Enable mode.
- SSH—SSH username and password.
- SSH Enable Mode User Name and Password—SSH username and password in Enable mode.

You can update these credentials using **Inventory > Device Administration > Add / Import / Manage Devices**.

The command syntax for `cwcli inventory cda` is:

`cwcli inventory cda -u` *userid* `-p` *password* {`-invoke` | `-status`} [`-credType` *credTypeL*ist] {`-device` *list* | `-view` *name* | `-device` *list* `-view` *name* | `ipaddress` *list*} [`-d` *debuglevel*] [`-m` *email*] [`-help`] [`-l` *logfile*]

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to `cwcli inventory cda` command.

The other common arguments used by `cwcli export` are explained in Using the cwcli export Command

:

Argument	Description	Usage Notes
{`-invoke` | `-status`}	Invoke—Invokes the Check Device Attribute operation. Status—Displays the check device attributes result.	Mandatory. These arguments are mutually exclusive. You cannot run `-invoke` and `-status` together. After using the `-invoke` argument to the check device attribute you must run the command again with -status argument to view the result. If you are checking the device credentials for same devices and for same set of credentials, then you can use `-invoke` argument only once. If you are checking the device credentials for different devices and different credentials then you must use `-invoke` argument first and then you must use `-status`.
{`-credType` *credTypeList*}	Enter the device credentials for which you want to view the status. You can use the following arguments to view the different credentials status: • 0 —Enter **0** to view all credentials status. • 1 — Enter **1** to view status for Read Community. • 2 — Enter **2** to view status for Write Community. • 3 — Enter **3** to view status for SNMP version 3 username and password. • 4 — Enter **4** to view status for Telnet username and password. • 5 — Enter **5** to view status for Telnet username and password in Enable mode. • 6 — Enter **6** to view status for SSH username and password. • 7 — Enter **7** to view status for SSH username and password in Enable mode. You can specify multiple arguments separated by comma to check multiple credentials	Mandatory. If you do not specify the credentials type, all credentials status are displayed.

Argument	Description	Usage Notes
Command Argument for Inventory CDA `createjob`		
{**-device** *comma_separated_devicelist* }|{**-view** *device_view_name*}	**-device** *comma_separated_devicelist* - Specify devices to be used for the job. The *comma_separated_devicelist* is list of devices. **-view** *device_view_name* Specify the device view to be used for the job. The *device_view_name* is the name of a device view.	Mandatory. These arguments are mutually exclusive. You cannot run **-device** and **-view** together. **cwcli inventory cda createjob -u** *Username* **-p** *Password* **-device** *Device 1, Device 2* |**-view** *device_view_name*, **-schedule** *Schedule* **-scheduletype** *Schedule Type*
[{**-schedule** *MM/dd/yyyy:HH:mm:ss* **-scheduletype** *Once* | *Daily* | *Weekly* | *Monthly* | *LastDayOfMonth* | *6hourly* | *12hourly*}]	You can specify the date and time as well as the frequency of the CDA job. • To specify the date and time when you want to run the CDA job, use the **schedule** option. • To specify the frequency of the job use the **scheduletype** option. You have to set both the **schedule** and **scheduletype** options for a scheduled job. You do not have to set the **schedule** and **scheduletype** for an Immediate job.	Optional. *scheduletype* can have any of the following values: • Once • 6hourly • 12hourly • Daily • Weekly • Monthly If the **schedule** option is not specified, the job will be created as an immediate job.
[**-input** *argFile*]	Input file containing the details of the subcommands to be used for a job creation.	Optional If you are specifying the argument file, you need not specify the arguments in the command line. **cwcli inventory cda -u** *admin* **-p** *admin* [**-input** *argFile*]
[**-description** *JobDescription*]	Gives details of the job.	*JobDescription* is a user-defined entry describing the job details.
[**-notificationmail** *comma_separated_email_list*]	Specify the e-mail addresses to which the configuration job will sends status notices.	Optional Separate multiple addresses with commas.

Argument	Description	Usage Notes
{`-credType` *credentialList*}	Enter the device credentials for which you want to create a job. You can use the following arguments to view the different credentials status: • 0 —Enter **0** to view all credentials status. (ALL). • 1 — Enter **1** to view status for Read Community. • 2 — Enter **2** to view status for Write Community. • 3 — Enter **3** to view status for SNMP version 3 username and password. • 4 — Enter **4** to view status for Telnet username and password. • 5 — Enter **5** to view status for Telnet username and password in Enable mode. • 6 — Enter **6** to view status for SSH username and password. • 7 — Enter **7** to view status for SSH username and password in Enable mode. You can specify multiple arguments separated by comma to check multiple credentials.	Mandatory If you do not specify the credentials type, all credentials status are displayed.
Command Argument for Inventory CDA `stopjob`		
{`-id` *Job ID*}	You can stop only one job at a time. You can stop a CDA job that is in scheduled as well as running state.	Mandatory Use this command to stop an Inventory CDA job that is scheduled. `cwcli inventory cda stopjob -u` *userid* `-p` *password* {`-id` *jobID*}
Command Argument for Inventory CDA `deletejob` and `jobdetails`		
{`-id` *Job IDs*}	You can delete more than one job at a time. Enter the Job IDs that you want to delete, separated by commas. You can list the details of more than one job at a time. Enter the Job IDs separated by commas.	Mandatory Inventory CDA deletejob command: `cwcli inventory cda deletejob -u` *userid* `-p` *password* {`-id` *jobID1*, *jobID2*..} Inventory CDA jobdetails command: `cwcli inventory cda jobdetails -u` *userid* `-p` *password* {`-id` *jobID1*, *jobID2*..}

Argument	Description	Usage Notes
Command Argument for `Inventory CDA listjobs`		
[`-jobstatus` *status*]	You can specify the status of the job. This can be: • All jobs • Running jobs • Completed jobs • Pending jobs.	Optional. `cwcli inventory cda listjobs -u` *Username* `-p` *Password* [`-jobstatus` *A, R, C, P*]
Command Arguments for Inventory CDA `jobresults`		
{`-id` *Job ID, Job ID*}	You can list the results of more than one job at a time. Enter the job IDs separated by commas.	`cwcli inventory cda jobresults -u` *Username* `-p` *Password* `-id` *"Job ID 1" , "Job ID 2" , "Job ID 3"*
[`-csvoutput` *filepath*]	You can specify the fully qualified pathname for saving the job results.	If you do not specify this argument, the job results appear in the console itself. If the specified path does not exist, the job results are stored in the default location. `cwcli inventory cda jobresult -u` *admin* `-p` *admin* {`-jobid` *jobID*} [`-csvoutput` *filepath*]

The Table 13-1 maps the device credentials that you have entered in the Device and Credentials (**Inventory > Device Administration > Add / Import / Manage Devices**) database and the credentials that appear in the
`cwcli inventory cda` command:

Table 13-1 Credentials Mapping

Credentials in Device and Credentials Database	Credentials displayed in `cwcli inventory cda`
Device Name	deviceName
SNMP V2C RO Community String	ro
SNMP V2C RW Community String	rw
SNMP V3 Username and Password	snmpv3
Primary Credentials Username	telnet
Primary Credentials Username and Primary Enable Password	telnetEnable
Primary Credentials Username	ssh
Primary Credentials Username and Primary Enable Password	sshEnable

Table 13-2 describes the Credential Verification Report Status messages:

Table 13-2 Understanding Credential Verification Report

Status Message	Description
OK	Check for device credentials completed. The device credentials data in the Device and Credential Repository matches the physical device credentials.
No authentication configured	Device was not configured with authentication mechanism (Telnet/LocalUsername/TACACS). LMS was able to use Telnet and log into the device successfully with out using the values entered in the Device and Credential Repository.
Incorrect	Check for device credentials completed. The device credentials data in the Device and Credential Repository does not match with the physical device credentials for one of the following reasons: • The device credentials data in Device and Credential Repository is not correct. • The device is unreachable or offline. • One of the interfaces on the device is down.
No Data Yet	Check for device credentials is in progress.
Did Not Try	Check for device credentials is not performed for one of the following reasons: • A Telnet password does not exist, so could not login to the device. • Device Telnet login mode failed, so enable mode login is not attempted.
No Value To Test	Check for device credentials is not performed because you have not entered the device credentials data.
Not Supported	Check for Telnet passwords is not performed because Telnet credential checking is not supported on this device.
Failed	Check failed because a Telnet session could not be established due to a not responding device.
Not Selected For Verification	Protocol was not selected for verification.

Usage Examples for cwcli inventory cda Command

This section provides some examples of usage for the **`cwcli inventory cda`** command.

Example 1: Invoking the Check Device Attributes

`cwcli inventory cda -u` *admin* **`-p`** *admin* **`-invoke -device`** 3750-stack

The command output is:

```
CDA invoked for given device and credType list
SUMMARY
========
        Successful: CDA: Success
```

Example 2: Checking the read and write device credentials for multiple devices

cwcli inventory cda -u admin **-p** admin **-device** 3750-stack, rtr% **-credtype** 1,2 **-status**

```
CDA Status :
============
deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnable
25 | rtr10005 | OK | OK |  |  |  |  |
27 | 3750-stack | OK | OK |  |  |  |  |
32 | rtr10K | No Data Yet | No Data Yet |  |  |  |  |
SUMMARY
========
        Successful: CDA: Success
```

Example 3: Checking all device credentials for a group

cwcli inventory cda -u admin **-p** admin **-view** "/RME@*ciscoworksservername*/Pre-deployed" **-status**

```
CDA Status:
==========
deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnable
29 | v2 | No Data Yet | No Data Yet | No Data Yet | No Data Yet | No Data Yet | No Data
Yet | No Data Yet
SUMMARY
========
        Successful: CDA: Success
```

Example 4: Checking device credentials for a device using the cwcli get request

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

Enter this in your browser:

http://ciscowork_servername:1741/rme/cwcli?command=cwcli inventory cda -u *admin* **-p** *YWRtaW4=* **-device** *10.10.10.12* **-status**

The output for this appears on your console:

```
<!-- Processing Starts  -->
CDA Status :
============
deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnable
12 | 10.10.10.12 | OK | OK | No Value To Test | Incorrect | Did Not Try | Failed | Did
Not Try
SUMMARY
========
Successful: CDA: Success
<!-- Processing complete -->
```

Example 5: Checking device credentials for a device using the cwcli post request

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, *cda.xml* contains:

```
<payload>
   <command>
     cwcli inventory cda -u admin -p YWRtaW4=  -device 10.10.16.20 -status
   </command>
</payload>
```

At the command prompt enter:

perl *samplepost.pl* **http://ciscowork_servername:1741/rme/cwcli** *cda.xml*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
<!-- Processing Starts  -->
CDA Status :
============
deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnab
le
71 | 10.10.16.20 | No Data Yet | No Data Yet | No Data Yet | No Data Yet | No
Data Yet | No Data Yet | No Data Yet

SUMMARY
========
        Successful: CDA: Success
<!-- Processing complete -->
```

Example 6: Creating a job using cwcli inventory cda createjob command

```
cwcli inventory cda createjob -u admin -p admin - Cat6230, Cat4500 | -view myview
-schedule 03/23/2007:12:15:01 -scheduletype Once
```

This command creates a cda job for the devices Cat6230 and Cat4500 in the view myview and scheduled for 23rd march 2007 at 12:15 pm with schedule type specified as Once.

Example 7: Stopping a cwcli inventory cda job using stopjob command

There is a job 1098, which is currently running. You can use this command to stop the job 1098.

```
cwcli inventory cda stopjob -u admin -p admin -id 1098
```

Example 8: Deleting cwcli inventory cda jobs using deletejob command

There are two jobs 1057 and 1058 scheduled. You can use this command to stop the two jobs.

```
cwcli inventory cda deletejob -u admin -p admin -id 1057,1058
```

Example 9: Getting details of jobs using cwcli inventory cda jobdetails command

There are two jobs 1001 and 1002 that are scheduled. You can use this command to list the details of both the jobs:

```
cwcli inventory cda jobdetails -u admin -p admin -id 1001, 1002
```

Example 10: Listing the cda jobs based on the status using the listjobs command

```
cwcli inventory cda listjobs -u admin -p admin -jobstatus R, C
```

Use this command to list those jobs whose status is Running or Completed.

Example 11: Obtaining results of jobs using jobresults comand

There are two jobs 1023 and 1024 that are completed. You can use this command to save the results of these jobs to the specified location.

```
cwcli inventory cda jobresult -u admin -p admin -jobid 1023, 1024 -csvoutput
C:/jobs/results
```

Running the cwcli inventory crmexport Command

You can use this command to export device credentials in CSV or XML format.

The command syntax for **cwcli inventory crmexport** is:

cwcli inventory crmexport -u *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] {**-device** *list* | **-view** *name* | **-device** *list* **-view** *name*} [**ipaddress** *list*] {**-filetype** *format* | **-filename** *outputfile*}

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to **cwcli inventory crmexport** command. The other common arguments used by **cwcli export** are explained in Using the cwcli inventory Command.

Argument	Description	Usage Notes
{**-filetype** *format* }	**-filetype** *format* —Enter the file format to export, either XML or CSV.	Mandatory. The default CSV file format version is 3.0.
{ **-filename** *outputfile* }	**-filename** *outputfile*—Enter the filename.	Mandatory. Specifies the name of the file to which the device credentials information is to be exported on LMS server. If you are using **cwcli** remotely (get or post request), by default the output file is available at this location on LMS server: On Windows: *NMSROOT*\MDC\tomcat Where, *NMSROOT* is the LMS installed directory. On Solaris and Soft Appliance: *NMSROOT*/objects/dmgt

Usage Examples for cwcli inventory crmexport Command

This section provides some examples of usage for the **cwcli inventory crmexport** command.

Example 1: Exporting device credentials of all devices in XML format

cwcli inventory crmexport -device *%* **-filetype** *xml* **-filename** *crmexport-xml* **-u** *admin* **-p** *admin*

```
SUMMARY
======== Successful: Export: Success
```

The device credentials are exported into a file, *crmexport-xml* in XML format. The credentials that are exported depends on the data that you have provided when you added the devices to Device Credentials Repository.

Example 2: Exporting device credentials of all devices in Normal State in CSV format

cwcli inventory crmexport -view "*/RME@ciscoworksservername/Normal Devices*" **-filetype** *csv* **-filename** *crmexport-csv* **-u** *admin* **-p** *admin*

```
SUMMARY
========
        Successful: Export: Success
```

The device credentials for devices that are in Normal state are exported into a file, *crmexport-csv* in CSV version 3.0 format. The credentials that are exported depends on the data that you have provided when you added the devices to Device Credentials Repository.

Example 3: Exporting device credentials of all devices using cwcli get request method

The password that you enter here must be in base64 encoded.

In this example,

- *YWRtaW4=* is the base64 encoded password for admin.
- %25 is the URL encode for "%"

Enter this in your browser:

http://*ciscowork_servername:***1741/rme/cwcli?command=cwcli inventory crmexport -u** *admin* **-p** *YWRtaW4=* **-device** *%25* **-filetype** *xml*
-filename *getxml*

The output is written in the *getxml* file. The *getxml* file is located:

On Windows:

NMSROOT\MDC\tomcat

Where, *NMSROOT* is the LMS installed directory.

On Solaris and Soft Appliance:

NMSROOT/objects/dmgt

Example 4: Exporting device credentials of all devices using cwcli post request method

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, *crmexport.xml* contains:

```
<payload>
   <command>
    cwcli inventory crmexport -u admin -p YWRtaW4=  -device 10.66.162.208 -filetype xml
-filename /opt/CSCOpx/crmexport-xml
```

```
   </command>
</payload>
```

At the command prompt enter:

perl *samplepost.pl* **http://ciscowork_servername:1741/rme/cwcli** *crmexport.xml*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
SUMMARY
========
        Successful: Export: Success
```

The device credentials are exported into a file, *crmexport-xml* in XML format. This file is created in the /opt/CSCOpx directory. By default, the specified file is created in this location:

On Windows:

NMSROOT\MDC\tomcat

Where, *NMSROOT* is the LMS installed directory.

On Solaris and Soft Appliance:

NMSROOT/objects/dmgt

The credentials that are exported depends on the data that you have provided when you added the devices to Device Credentials Repository.

Running the cwcli inventory deletedevice Command

You can use this command to delete devices.

The device information will be retained in the Device Credentials Repository. This information will not be removed till you delete the device from Device Credentials Repository.

The command syntax for **cwcli inventory deletedevice** is:

cwcli inventory deletedevice -u *userid* **-p** *password* [**-d** *debuglevel*]
[**-m** *email*] [**-l** *logfile*] [**-view** *name*] {**-device** *list* | **-input** *inputfile* | **ipaddress** *list*}

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to **cwcli inventory deletedevice** command. The other common arguments used by **cwcli export** are explained in Using the cwcli export Command.

Argument	Description	Usage Notes
-input *inputfile*	**-input** *inputfile*—Enter the full path of the file containing comma-separated list of device display name as entered in Device Credentials Repository. The input file should be of this format: **-device** 1.1.1.1,2.2.2.2,3.3.3.3 or **-device** 1.1.1.1 **-device** 2.2.2.2 **-device** 3.3.3.3	Mandatory You must also enter the file format either CSV or txt.

Usage Examples for cwcli inventory deletedevice Command

This section provides some examples of usage for the **cwcli inventory deletedevice** command.

Example 1: To delete a device

cwcli inventory deletedevice -u *admin* **-p** *admin* **-device** *10.76.10.10*

```
<cwcli> INFO - Total number of devices deleted successfully: 1
SUMMARY
========
        Successful: Delete Device: Success
```

Example 2: To delete devices listed in a file

The input file, deletedevice contains list of device Display Name separated by a comma:

-device 3750-stack,rtr1000,rtr10005

cwcli inventory deletedevice -u *admin* **-p** *admin* **-input** *deletedevice.csv*

Example 3: To delete devices using cwcli get request

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

Enter the following in your browser:

http://ciscowork_servername:1741/rme/cwcli?command=cwcli inventory deletedevice -u *admin* **-p** *YWRtaW4=* **-device** *10.10.10.41,10.10.10.51*

The output for this appears on your console:

```
<!-- Processing Starts  -->
<cwcli> INFO - Total number of devices deleted successfully: 2
SUMMARY
========
        Successful: Delete Device: Success
<!-- Processing complete -->
```

Example 4: To delete devices using cwcli post request

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

The payload file, *deletedevicestate.xml* contains:

```
<payload>
   <command>
     cwcli inventory deletedevice -u admin -p YWRtaW4=  -device
10.77.9.10,10.77.9.18,10.76.8.6
   </command>
</payload>
```

At the command prompt enter:

perl *samplepost.pl* **http://doclab2:1741/rme/cwcli** *deletedevice.xml*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
<!-- Processing Starts  -->
<cwcli> INFO - Total number of devices deleted successfully: 3


SUMMARY
========
        Successful: Delete Device: Success
<!-- Processing complete -->
```

Running the cwcli inventory getdevicestate Command

You can use this command to view the device state.

The command syntax for **cwcli inventory getdevicestate** is:

cwcli inventory getdevicestate -u *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] [**-view** *name*] {**-device** *list* | **-input** *inputfile* | **ipaddress** *list*}

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to **cwcli inventory getdevicestate** command. The other common arguments used by **cwcli export** are explained in Using the cwcli inventory Command.

Argument	Description	Usage Notes
-input *inputfile*	**-input** *inputfile*—Enter the full path of the file containing comma-separated list of devices display name as entered in Device Credentials Repository. The input file should be of this format: **-device** 1.1.1.1,2.2.2.2,3.3.3.3 or **-device** 1.1.1.1 **-device** 2.2.2.2 **-device** 3.3.3.3	Mandatory You must also enter the file format either CSV or txt.

Usage Examples for cwcli inventory getdevicestate Command

This section provides some examples of usage for the **cwcli inventory getdevicestate** command.

Example 1: To view the device state of the devices

cwcli inventory getdevicestate -u *admin* **-p** *admin* **-device** *10.10.19.10,10.10.19.12*

```
<cwcli> INFO - Device State Information
DisplayName:Device State
10.10.19.10:PREDEPLOYED
10.10.19.12:NORMAL
SUMMARY
========
        Successful: getdevicestate: Success
```

Example 2: To view the devices state specified in a file

The input file, deletedevice contains list of device Display Name separated by a comma:

-device VG200,rtr1750,cat4000

cwcli inventory deletedevice -u *admin* **-p** *admin* **-input** *devicestate.csv*

Example 3: To view the devices state using get request

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

Enter the following in your browser:

http://ciscowork_servername:1741/rme/cwcli?command=cwcli inventory getdevicestate -u *admin* **-p** *YWRtaW4=* **-device** *10.16.10.15,10.16.10.35*

The output for this appears on your console:

```
<!-- Processing Starts  -->
<cwcli> INFO - Device State Information
DisplayName:Device State
```

```
10.16.10.15:NORMAL
10.16.10.35:PREDEPLOYED

SUMMARY
========
        Successful: getdevicestate: Success
<!-- Processing complete -->.
```

Example 4: To view the device state using post request

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, *getdevicestate.xml* contains:

```
<payload>
   <command>
     cwcli inventory getdevicestate -u admin -p YWRtaW4=  -device
12.20.12.26,10.6.12.21,12.18.10.129,10.7.9.13
   </command>
</payload>
```

At the command prompt enter:

`perl` *samplepost.pl* **`http://ciscowork_servername:1741/rme/cwcli`** *getdevicestate.xml*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
<!-- Processing Starts  -->
<cwcli> INFO - Device State Information
DisplayName:Device State
12.18.13.129:ALIAS
10.7.9.13:PREDEPLOYED
10.6.12.21:NORMAL
12.20.12.26:NORMAL

SUMMARY
========
        Successful: getdevicestate: Success
<!-- Processing complete -->
```

Sample Script to Invoke the Servlet

```
#!/opt/CSCOpx/bin/perl
use LWP::UserAgent;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
print "\n argv[0} = $ARGV[0] , fname = $fname \n";
open (FILE,"$fname") || die "File open Failed $!";
while ( <FILE> )
{
$str .= $_ ;
}
#print $str ;
url_call($temp);
#-- Activate a CGI:
```

```
sub url_call
{
my ($url) = @_;
my $ua = new LWP::UserAgent;
$ua->timeout(1000);
# you can set timeout value depending on number of devices
my $hdr = new HTTP::Headers 'Content-Type' => 'text/html';
my $req = new HTTP::Request ('GET', $url, $hdr);
$req->content($str);
print "It comes here \n";
my $res = $ua->request ($req);
my $result;
#    print "It comes here too \n";
if ($res->is_error)
{
print "ERROR : ", $res->code, " : ", $res->message, "\n";
$result = '';
}
else {
    $result = $res->content;
       if($result =~ /Authorization error/)
{           print "Authorization error\n";
          }
else {
print "\n $result" ;
         }
     }
}
```

Overview: cwcli invreport Command

The **cwcli invreport** is a CiscoWorks command line tool which allows you to run previously created Inventory Custom Reports and also system reports. The supported output file format is Comma Separated Value (CSV).

The above command retrieves the inventory report in CSV format. The **-file** parameter stores the output in the file specified by *filename*. If you have not specified the filename, the output is stored at the following location:

- *NMSROOT*\files\rme\cri\archives\inventory*reportname_timestamp*.csv (On Windows)
- /var/adm/CSCOpx/files/rme/cri/archives/inventory/*reportname_timestamp.csv* (On Solaris and Soft Appliance)

NMSROOT is the LMS install directory.

You can:

- Use the **-reportname** argument to generate the report.

  This can be the name of:

  – An already defined custom template

  or

  – A system report name such as Detailed Device Report.

- Use the **-input** argument to specify a file containing the parameters for the report generation.

Note The **-view** argument is not allowed in the input file.

- Enable debug mode and set the debug level using the `-d` argument.
- E-mail the output to an e-mail recipient using the `-m` argument.
- Log the error messages to a file using the `-l` argument. The log and the output files are created in the current directory.
- List the existing reports with the `-listreports` argument.

Running the cwcli invreport Command

To use the `cwcli invreport` command, you must be able to run the cwcli command

You should be authorized to generate inventory reports.

The command syntax is:

`cwcli invreport -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*] [`-l` *logfile*] {`-listreports` | `-reportname` *name* {`-view` *viewname* | `-device` *list* | `-ipaddress` *list*} [`-file` *filename*] | `-input` *inputfile*}

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used. Valid values for arguments are described in the following table:

Argument	Description	Usage Notes
`-u` *user*	Provide valid LMS username.	None.
`-p` *password*	Provide password for username. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.	None.
[`-d` *debug_level*]	Set debug level.	Optional. *debug_level* is a number between 1 (the least information is sent to the debug output) and 5 (the most information is sent to the debug output). If you do not specify this argument, 4(INFO) is the default debug level.
[`-m` *email*]	Specify an e-mail address to send the results.	Optional. *email* is one or more e-mail addresses for notification. They can be separated by a space or comma.
[`-l` *log_filename*]	Logs the error messages and debug of messages of the invreport command, to the specified logfile name. If not specified, it will be written to default logs (invreports.log and cli.log).	Optional. *log_filename* can be full pathname or filename in local directory.

Argument	Description	Usage Notes
[`-l` *log_filename*]	Logs the error messages and debug of messages of the invreport command, to the specified logfile name. If not specified, it will be written to default logs (invreports.log and cli.log).	Optional. *log_filename* can be full pathname or filename in local directory.

Argument	Description	Usage Notes
{`-listreports` | `-reportname` *name* {`-view` *viewname* | `-device` *list* | `-ipaddress` *list*} [`-file` *filename*] | `-input` *inputfile*}	Specify any one of the required arguments: • `-listreports` • `-reportname` • `-input`	`-listreports` argument lists out all Inventory system reports and custom reports templates. You can run this command if you have the required permissions to generate reports. `-reportname` *name* specifies the name of an already defined custom template or the name of a system report (such as Detailed Device Report) for which the CSV formatted report is to be generated. `-input` *inputfile* specifies the input file containing report parameters. The parameters in this file will be used to generate the CSV formatted report(s). For Solaris and Soft Appliance, you must specify the complete path of the input file. For Windows, this file should be located in the current directory or you can specify the complete path of the input file. The `-view` argument is not allowed in the input file.

Argument	Description	Usage Notes
	If you selected `-reportname` *name*, then specify any one of these arguments: – `-view` *viewname*. This confines the device search to the specified view. – `-device` *list.* This specifies one or more device names as a comma-separated list. Optionally, you can also specify `-file` *filename.* Name of the file where CSV formatted report will be stored. If you do not specify the location, the default location is: *NMSROOT*\files\rme\cri\archives\inventory*reportname_timestamp.csv* (On Windows) /var/adm/CSCOpx/files/rme/cri/archives/inventory/*reportname_timestamp.csv* (On Solaris and Soft Appliance) – `ipaddress` *list*—This specifies IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated. You cannot use this option with `-device`, `-view` , or `-input`. Also, you cannot specify wildcard characters.	

Usage Examples

This section provides some examples of usage for the cwcli invreport command:

- Example 1
- Example 2
- Example 3
- Example 4
- Example 5
- Example 6

Example 1

`cwcli invreport -u` *admin* `-p` *admin* `-reportname` *"Detailed Device Report"* `-device` %

This generates Detailed Device Report for all devices and CSV file will be located at

- *NMSROOT*\files\rme\cri\archives\inventory*Detailed Device Report_timestamp.csv* (On Windows)
- /var/adm/CSCOpx/files/rme/cri/archives/inventory/*Detailed Device Report_timestamp.csv.* (On Solaris and Soft Appliance)

Example 2

cwcli invreport -u *admin* **-p** *admin* **-reportname** *"Detailed Device Report"* **-device** % **-file** *D:\cisco\CSCOpx\a.csv*

This generates Detailed Device Report, a system report, for all devices, and the result will be written to D:\cisco\CSCOpx\a.csv

Example 3

cwcli invreport -u *admin* **-p** *admin* **-reportname** *"Detailed Device Report"* **-device** % **-file** a.csv

This generates the Detailed Device Report, a system report, for all devices, and the result will be written to the file a.csv in the current directory (from where you are running this command).

Example 4

cwcli invreport -u *admin* **-p** *admin* **-input** *cliinputs.txt*

Generate the reports using the parameters provided in the file cliinputs.txt. Using **-input** argument you can run multiple reports at a time by providing parameters in the file.

Example 5

cwcli invreport -u *admin* **-p** *admin* **-listreports**

Displays a list of all Inventory system report and custom templates.

You can run this command if you have the required permissions to generate reports.

Example 6

cwcli invcreport -u *admin* **-p** *admin* **-d** 3 **-m** *xxx@yyy.com* **-reportname** *acmeinventory* **-view** acme **-file** *acmeinventory.txt*

Generates the report named acmeinventory, using the acme device view and the CSV formatted output will be written to acmeinventory.txt

You can place this file in the current directory (from where you are running the command).

Example 7

cwcli invreport -u *admin* **-p** *admin* **-reportname** *HardwareStatisticsReport* **-device** *devname* **-file** *hwstreport.txt*

Generates the Hardware Statistics Report for the device devname and the CSV formatted output will be written to hwstreport.txt

Example 8

cwcli invreport -u *admin* **-p** *admin* **-reportname** *DeviceStatisticsReport* **-device** *devname* **-file** *devstreport.txt*

Generates the Device Statistics Report for the device devname and the CSV formatted output will be written to devstreport.txt

Example 9

cwcli invreport -u *admin* **-p** *admin* **-reportname** *POEReport* **-device** *devname* **-file** *report.txt*

Generates the POE Report for the device devname and the CSV formatted output will be written to report.txt

cwcli invreport Remote Access

You can also perform the **cwcli invreport** tasks using the servlet. You will have to upload a payload XML file, which contains the **cwcli invreport** command arguments and LMS user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to execute any command:

For post request,

perl *samplepost.pl* **http://***lms-server:lms-port***/rme/cwcli** *payload_XML_file*

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

perl *samplepost.pl* **https://***lms-server:lms-port***/rme/cwcli** *payload_XML_file*

The default port for LMS server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>
<command>
cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...
</command>
</payload>
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

For get request,

`http://`*lms-server:rme-port*`/rme/cwcli?command=cwcli invreport`** *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

The default port for LMS server in HTTP mode is 1741.

If you have enabled SSL on LMS server, you can also use https protocol for secured connection.

`https://`*lms-server:lms-port*`/rme/cwcli?command=cwcli invreport`** *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

The default port for LMS server in HTTPS mode is 443.

The BAse64 encoded for “admin” is YWRtaW4=.

The URL encode for,

- Double quotes (“) is %22
- Percentage sign (%) is %25

Overview: cwcli netshow Command

You can invoke NetShow features from Command Line Interface (CLI).

The **`cwcli netshow`** commands let you use NetShow features from the command line. You can use the **`cwcli netshow`** commands to view, browse, create, delete, and cancel NetShow jobs.

You can also view the Command Sets assigned to each user by entering the command **`listcmdsets`** from CLI.

You can set the following job attributes using the command line option:

- E-mail Notification
- Job Based Password
- Execution Policy
- Approver List

However, the Administrator must define and assign the command sets to you, in the browser interface.

If you do not have permission to run custom commands, you can run a command or command set from the CLI only if:

- The command set is assigned to you by the Administrator.
- The command set has at least one command that can be run on the specified device.

If you have permission to run custom commands, you can run any of the following adhoc commands:

- **`show`**
- **`version`**
- **`where`**
- **`ping`**
- **`traceroute`**
- **`?`**

Administrator level users have all command sets assigned to them. However, only system-defined command sets are assigned to all users, by default. Other commands have to be assigned to the user by the Administrator. If any users create a command, it is automatically assigned to them.

Running cwcli netshow Command

The command syntax for running **cwcli netshow** commands is:

cwcli netshow *common_arguments subcommands command_arguments*

In the CLI version, you can provide the arguments in the (operating system shell) command line or in an input file. The input file provides you with flexibility and control over commands and command sets. You can specify the devices on which you want to run the command sets.

In the input file, you can include subcommands and command arguments.

For example, you can create a new netshow job with command sets, set1 and set2, and the custom commands, custom command 1 and custom command 2, by entering:

cwcli netshow createjob -u *Username* **-p** *Password* **-commandset** "*Command Set 1*"," *Command Set 2*" **-device** *Device 1, Device 2* **-customcmd** "*Custom command 1*"," *Custom command 2*" **-schedule** *Schedule* **-scheduletype** *Schedule Type*

Items in square brackets ([]) are optional; items in curly brackets ({}) are required.

The arguments are described in the following sections.

Subcommands

Subcommands specify the actions that you perform. Valid values for subcommands are described in the following table.

Sub Command	Description	Usage Notes	Example
createjob	Creates a new job that can be scheduled to run immediately or to be run sometime in the future. You can also specify the job attributes you want to enable.	Either use an input file containing the details of the subcommands or enter the full command syntax.	**cwcli netshow createjob -u** *Username* **-p** *Password* **-commandset** "*Command Set 1*"," *Command Set 2*" **-device** "*Device Name 1*", "*Device Name 2*" **-customcmd** "*Custom Command 1*", "*Custom Command 2*" **-schedule** *Schedule* **-scheduletype** *Schedule Type* Or **cwcli netshow createjob -u** *Username* **-p** *Password* **-input** *Input File*
canceljob	Cancels an existing job.	Enter the job ID.	**cwcli netshow canceljob -u** *Username* **-p** *Password* **-id "***Job ID***"**
deletejob	Deletes existing jobs.	Enter the job IDs separated by commas.	**cwcli netshow deletejob -u** *Username* **-p** *Password* **-id** "*Job ID 1*"," *Job ID 2*"
jobdetails	Displays details of specified job.	Enter the job IDs separated by commas.	**cwcli netshow jobdetails -u** *Username* **-p** *Password* **-id** "*Job ID 1*","*Job ID 2*", "*Job ID 3*"

`listjobs`	Displays a list of jobs created by the user and the job status.	Specify the type of jobs to be listed. The command type is case sensitive. The commands that you can use are: `A` —All jobs `R` —Running jobs `C` —Completed jobs `P` —Pending jobs You can use combinations of status options. Separate the options by commas.	`cwcli netshow listjobs -u` *Username* `-p` *Password* `-status` *R,C*
`listcmdsets`	Displays a list of command sets assigned to the user.	None.	`cwcli netshow listcmdsets -u` *Username* `-p` *Password*
`jobresults`	Displays results of specified jobs	Specify the job IDs. Separate the job IDs by commas.	`cwcli netshow jobresults -u` *Username* `-p` *Password* `-id` *"Job ID 1" , "Job ID 2" , "Job ID 3"*
`help`	Displays command usage information.	None.	`cwcli netshow -help`

Common Arguments

Common arguments specify parameters that apply to all subcommands. Valid values for *common_arguments* are described in the following table.

Command	Description	Usage Notes
`-u` *user*	Enter a valid LMS username.	None
`-p` *password*	Enter the password for the username. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.	None
`[-d` *debug_level*`]`	Set the debug level.	Optional *debug_level* should be a number between 1-5. 1 —The least information is sent to the debug output 5 —The most information is sent to the debug output.
`[-l` *log_filename*`]`	Identifies a file to which Network Show Commands will write log messages. If you do not specify this, the log output will appear on screen.	Optional *log_filename* can be a full path to the file or a filename in the local directory.
`[-m` *Email ID*`]`	Enter your Email ID	You will get the output of the CLI operation in an Email.

Command Arguments

Command arguments specify parameters that apply only to specific subcommands. Valid values for command arguments are described in the following table.

Arguments in square brackets ([]) are optional. Arguments in curly brackets ({}) are required. You must provide one argument from each group of arguments in curly brackets ({}) that is separated by vertical bars (|).

Command Arguments	Description	Usage Notes
Command Arguments for `createjob`		
{**`-device`** *devicelist* | **`-view`** *view_name*}	Defines devices on which you want the command set to run.	*device_list* —List of device names. Separate these names by commas. *view_name* — Name of a device view.
{**`-commandset`** *commandset*}	Defines available command sets that you want to run on the selected devices.	*commandset* is the name of the command set that was assigned to you. You can specify more than one command set separated by commas. The command set name is case sensitive. You must specify *command set* or *custom command* or both to create a job.
{**`-customcmd`** *customcommand*}	Defines the user-defined commands that you want to run on the selected devices.	*customcommand* is a user-defined show command. You must specify *command set* or *custom command* or both to create a job. The custom commands which can be run on NetShow are: • **`show`** • **`version`** • **`where`** • **`ping`** • **`traceroute`** • **`?`** You can use the short forms of these commands. For example, **`sh`** for **`show`**.
[**`-description`** *description*]	Gives details of the job.	*description* is a user-defined entry describing the job details.

Command Arguments	Description	Usage Notes
[{**-schedule** *MM/dd/yyyy:HH:mm:ss* **-scheduletype** *Once* | *Daily* | *Weekly* | *Monthly* | *LastDayOfMonth* | *6hourly* | *12hourly*}]	You can specify the date and time as well as the frequency of the NetShow job. • To specify the date and time when you want to run the NetShow job, use the schedule option. • To specify the frequency of the job use the scheduletype option. You have to set both the schedule and schedule type options for a scheduled job. You do not have to set the schedule and schedule type for an Immediate job.	*scheduletype* can have any of the following values: • Once • 6hourly • 12hourly • Daily • Weekly • Monthly • LastDayOfMonth If the schedule option is not specified, the job will be created as an immediate job.
[**-makercomments** *comments*]	Job creator's comments to Job approver.	
[**-mkemail** *email*]	Maker e-mail ID for sending approval notifications	
[**-notificationmail** *email]*	Defines the e-mail addresses of persons who need to get mails when the job has started and completed.	*email* can contain a comma separated email list. If you do not specify this option in the CLI, the e-mail address specified in the UI are used.
[**-execution** *Sequential*|*Parallel*]	Execution policy. Specifies the order in which you want to run the job on the devices. Parallel—Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time. Sequential—Allows the job to run on only one device at a time.	If you do not specify these options in the CLI, the corresponding settings from the UI are used.
{**-primary_user** *username* **-primary_pass** *password*}	Primary username and password to connect to devices.	
{**-enable_pass** *password*}	Execution mode password to connect to device.	
[**-input** *input file*]	Input file containing the details of the subcommands	If you are specifying the input file, you do not need to specify the subcommands.

Command Arguments	Description	Usage Notes
Command Argument for `listjob`		
{`-status` *status*}	You can specify the status of the job. This can be: • All jobs • Running jobs • Completed jobs • Pending jobs.	
Command Argument for `canceljob`		
{`-id` *Job ID*}	You can cancel only one job at a time.	
Command Argument for `deletejob` and `jobdetails`		
{`-id` *Job ID, Job ID}*	You can delete more than one job at a time. Enter the Job IDs that you want to delete, separated by commas. You can list the details of more than one job at a time. Enter the Job IDs separated by commas.	
Command Arguments for `jobresults`		
{`-id` *Job ID, Job ID*}	You can list the results of more than one job at a time. Enter the job IDs separated by commas.	
[`-output` *file path*]	You can specify the fully qualified pathname for saving the job results.	If you do not specify this argument, the job results appear in the console itself. If the specified path does not exist, the job results are stored in the default location.

Executing Netshow CLI Remotely

You can run NetShow CLI from a remote console.

NetShow uses the Remote Access feature in the CLI framework to help you to invoke the NetShow commands from the client in the same way as you run them on the LMS server.

The name of the servlet, to be invoked, is /rme/cwcli.

You must invoke the following URLs to run any command.

- For POST request:

  `http://`*lms-server:lms-port*/rme/`cwcli` *payload XML file*

- For GET request:

  `http://`*lms-server:lms-port*/rme/cwcli?command=`cwcli netshow` *command* `-u` *Username* `-p` *Password command_specific_args*

The contents of the payload.xml is:

```
<payload>
   <command>
    cwcli netshow command -u Username -p Password command_specific_args
   </command>
</payload>
```

For example to run the **listcmdsets** command payload.xml will be as follows:

```
<payload>
<command>
cwcli netshow listcmdsets -u Username -p Password
</command>
</payload>
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

Performance Tuning Tool

Performance Tuning Tool (PTT) is a Command Line Interface (CLI) utility that enables you to apply and list various profiles available in LMS server. Profiles consists of configuration files, which are in the form of XML files whose values are based on the recommendations for various applications. For more information on PTT features, refer to PTT Features.

There are two profiles shipped with LMS. You can use any of the profile that matches the system. For more information on PTT Profiles, see Profiles and PTT.

There maybe multiple configuration files that are involved while applying a profile. The parameters such as, snmp.threads.min, snmp.threads.max, ICSThreadCount, ICS DBConnectionCount, ThreadPoolCount, CDLNumOfThreads, max_db_connections, max_threads_for_config_fetch, EssentialsDMServicesHeapsize,ConfigJobManager.heapsize, and CDA_MIN_THREADS are tuned and available in each profile. You can apply the required profile to the system and improve performance. This is a major advantage of using PTT.

To know more about the command usage, see PTT Commands.

PTT Features

The PTT CLI utility allows you to:

- List the profile that is currently applied to the target machine.
- List the profiles that match the system configuration.
- List the profiles that match the operating system.
- Apply a selected profile onto the target machine.
- Reverse the changes done to a target machine by applying the default profile to restore the default settings.
- View details of a profile.

Profiles and PTT

Profiles are XML files whose values are based on the recommendations of the various LMS applications. Each profile (XML file) consists of tuned parameters which when applied, improves performance.

There are two profiles that are shipped with LMS. They are:

- Default Profile
- Perftune - Windows and Perftune - Solaris and Soft Appliance

Note All the configuration files are backed up before applying a profile.

PTT identifies the matching profile for a LMS server based on the following criteria:

- The operating system for which the profile is created.
- The System Configurations such as Dual CPU and 4 GB RAM.

A profile is considered matching only if it meets these criteria.

When you apply a profile, the tuned parameters, see Table 13-3 corresponding to that profile is applied to the system.

These parameters belong to Sync Archive, Netconfig, Syslog, Device Management, Check Device Attributes (CDA) and Inventory Collection sub systems of the LMS application. The profile, with tuned parameters when applied, improves the performance. Before running PTT, ensure that the Daemon manager is stopped.

Default Profile

A default profile is a profile with default values. It is used to rollback the changes done by PTT. You can roll back the changes made to a profile, by applying the default profile. This action rolls back the parameters to their original values. The parameters and the original values are:

Table 13-3 Default Profile Original Values

Sub system	Parameters	Original Values	Platform Supported
CDA	CDA_MIN_THREADS	7	Windows and Solaris and Soft Appliance
EssentialsDM	ConfigJobManager.heapsize	192m	Windows and Solaris and Soft Appliance
EssentialsDM	EssentialsDMServiceHeapsize	256	Windows and Solaris and Soft Appliance
Inventory Collection	snmp.threads.min	10	Windows and Solaris and Soft Appliance
Inventory Collection	snmp.threads.max	15	Windows and Solaris and Soft Appliance
Inventory Collection	ICS ThreadCount	10	Windows and Solaris and Soft Appliance
Inventory Collection	ICS DBConnectionCount	5	Windows and Solaris and Soft Appliance
NetConfig and SyncArchive	max_threads_for_config_fetch	5	Windows and Solaris and Soft Appliance

Table 13-3 Default Profile Original Values

Sub system	Parameters	Original Values	Platform Supported
NetConfig and SyncArchive	ThreadPoolCount	10	Windows and Solaris and Soft Appliance
NetConfig and SyncArchive	CDLNumOfThreads	5	Windows and Solaris and Soft Appliance
NetConfig and SyncArchive	max_db_connections	20	Windows and Solaris and Soft Appliance
Config Management (Config Management Server Daemons - dmgtd.conf Arguments for max heap size.)	Xmx	192	Solaris and Soft Appliance
Config Management (Config Management Server Daemons - dmgtd.conf Arguments for minimum heap size.)	Xms	64	Solaris and Soft Appliance

Perftune - Windows and Perftune - Solaris and Soft Appliance

This profile consists of parameters that are tuned to improve performance.

- Perftune - Windows profile is applied to a system that has a Windows operating system, provided the profile matches the required criteria.
- Perftune - Solaris and Soft Appliance profile is applied to a system that has a Solaris and Soft Appliance operating system, provided the profile matches the required criteria.

  See Profiles and PTT for more informationon criteria for a profile to match a system.

The parameters that can be tuned are:

Table 13-4 Perftune - Windows and Perftune - Solaris and Soft Appliance Parameters

Sub system	Parameters	Original Values	New Value	Platform Supported
CDA	CDA_MIN_THREADS	7	14	Windows and Solaris and Soft Appliance
EssentialsDM	ConfigJobManager.heapsize	192m	256	Windows and Solaris and Soft Appliance
EssentialsDM	EssentialsDMServiceHeapsize	256	512	Windows and Solaris and Soft Appliance
Inventory Collection	snmp.threads.min	10	20	Windows and Solaris and Soft Appliance
Inventory Collection	snmp.threads.max	15	25	Windows and Solaris and Soft Appliance
Inventory Collection	ICS ThreadCount	10	20	Windows and Solaris and Soft Appliance

Table 13-4 Perftune - Windows and Perftune - Solaris and Soft Appliance Parameters

Sub system	Parameters	Original Values	New Value	Platform Supported
Inventory Collection	ICS DBConnectionCount	5	10	Windows and Solaris and Soft Appliance
NetConfig and SyncArchive	max_threads_for_config_fetch	5	10	Windows and Solaris and Soft Appliance
NetConfig and SyncArchive	ThreadPoolCount	10	20	Windows and Solaris and Soft Appliance
NetConfig and SyncArchive	CDLNumOfThreads	5	20	Windows and Solaris and Soft Appliance
NetConfig and SyncArchive	max_db_connections	20	40	Windows and Solaris and Soft Appliance
Config Management (Config Management Server Daemons - dmgtd.conf Arguments for max heap size.)	Xmx	192	256	Solaris and Soft Appliance
Config Management (Config Management Server Daemons - dmgtd.conf Arguments for minimum heap size.)	Xms	64	128	Solaris and Soft Appliance

Example 1

If the Perftune - Windows profile is applied to a system which already has a default profile applied, the parameters are changed from the original values to new values. See Table 13-4 for Original and New values.

Example 2

If the default profile is applied to a system which already has a Perftune - Windows profile applied to it, the parameters are rolled back to original values. See Table 13-3 for Original values.

PTT Commands

Table 13-5 lists the various PTT command options that you can use. These command options are common for Windows and Solaris and Soft Appliance.

Table 13-5 PTT Command Options

PTT command options	Description
`-apply <profileName>`	Applies a particular profile. To reset, specify the default profile name as parameter and apply that profile.
`-apply`	Finds the matching profile and applies it automatically in a single step.
`-apply Default`	Finds the default profile and applies it automatically in a single step.
`-show`	Displays the currently applied profile.
`-list`	Lists all the profiles that match the target operating system.

PTT command options	Description
`-list Match`	Lists the profile that matches the system configuration.
`-view <profileName>`	Displays the profile details. The details of the profile, which is specified in the command is displayed.
`rmeptt -help`	Displays help for all commands.

Command Usage

In Windows enter:

`rmeptt.bat <option> <argument>`

For example, to list all the profiles that matches the target operating system, the command is:

`rmeptt.bat -list`

In Solaris and Soft Appliance, enter:

`rmeptt.sh <option> <argument>`

For example to display the profile details, the command is:

`rmeptt.sh -view x`

Where *x* is the name of the profile.

syslogConf.pl Utility

The syslogConf.pl is a perl script CLI utility. You can use this utility to:

- Change Syslog Analyzer Port.
- Change Syslog Collector Port.
- Configure Remote Syslog Collector (RSAC) Address and Port in LMS server.
- Change Syslog File Location.

You can run this script in the LMS server as well as the RSAC server. All the activities mentioned above can be performed in a LMS server by running the syslogConf.pl script from the command prompt.

In RSAC server, you can only change the Syslog Collector Port and Syslog File location. The Syslog Collector and Syslog Analyzer ports can be any number between 1025 and 5000.

This utility is available under:

NMSROOT/bin/ (On Solaris and Soft Appliance)

NMSROOT\bin (On Windows)

NMSROOT is the LMS install directory. For Solaris and Soft Appliance, it will be /opt/CSCOpx.

A log file for the syslogconf.pl script is available at:

In Solaris and Soft Appliance

/var/adm/CSCOpx/log/SyslogConf.log

In Windows

NMSROOT\log\SyslogConf.log

Note Before you run the syslogConf.pl script, ensure that the Daemon Manager is stopped.

Running the syslogConf.pl Script

To run the script:

Step 1 Go to the command prompt and enter:

```
NMSROOT/bin/perl NMSROOT/syslogConf.pl
```

When you run this syslogConf.pl script, a message appears with five options.

```
[1] Change Syslog Analyzer Port
[2] Change Syslog Collector Port
[3] Configure Remote Syslog Collector(RSAC) Address and Port
[4] Change Syslog File Location
[Q] Quit
Enter Your Choice:
```

Step 2 Enter your choice.

- If you enter **1** the following message is displayed with the old Syslog Analyser Port number. You are also prompted to enter the new port number for the Syslog Analyser.

  ```
  INFO: You have opted to change Local Syslog Analyser port.
  Old Syslog Analyser Port :xxxx
  Enter new Syslog Analyser port:
  ```

  For example, you can change the Syslog Analyser Port from 4444 to 2222.

  After providing the new port information, the following message is displayed.

  ```
  INFO:Local Syslog Analyser port has been changed from 4444 to 2222 successfully
  ```

- If you enter **2** the following message is displayed with the old Syslog Collector Port number. You are also prompted to enter the new port number for the Syslog Collector.

  ```
  INFO: You have opted to change Local Syslog Collector port.
  Old Syslog Collector Port :xxxx
  Enter new Syslog Collector port:
  ```

  For example you can change the Syslog Collector Port from 1111 to 3333.

  After providing the new port information, the following message is displayed.

  ```
  INFO:Local Syslog Collector port has been changed from 1111 to 3333 successfully
  ```

- If you enter **3**, the following message is displayed, with the old Syslog Collector Port number. You are also prompted to provide the new RSAC Address and the new port number for the Syslog Collector.

  ```
  INFO: You have opted to change RSAC port.
  Enter the RSAC Address:
  Old Syslog Collector Port :0
  Enter new Syslog Collector port:
  ```

  Ensure that the RSAC port that you configure in the LMS server corresponds with the Collector port configured in the RSAC server.

  You can specify srme-w2k as the RSAC Address, and change the Syslog Collector port from 0 to 3456.

After providing the RSAC Address and port information, the following message is displayed.

```
INFO: Remote Syslog Collector(RSAC) port has been changed from 0 to 3456.
```

- If you enter **4**, the following message is displayed with the old Syslog Directory Path. You are also prompted to enter the new Syslog Directory path.

  ```
  INFO: You have opted to change Syslog File Location
  Old Syslog Directory : /var/log/
  Enter Full Path of New Syslog Directory:
  ```

  Ensure that you enter the full directory path, if you are running the syslogConf.pl script on Solaris and Soft Appliance. You can provide the relative directory path if you are running the syslogConf.pl script on Windows.

  For example you can change the Syslog Directory location from /var/log/ to /var/log/newSyslogLoc.

  After providing the required information, the following message is displayed.

  ```
  Syslog file location changed from: /var/log/ to: /var/log/newSyslogLoc
  ```

- If you enter **Q,** you are allowed to quit from the script.

Software Management CLI Utility

You can invoke Software Management (SWIM) features from Command Line Interface (CLI).

The **`cwcli swim`** commands let you use SWIM features from the command line. You can use the **`cwcli swim`** commands to:

- List Images from Software Management (SWIM) Repository
- Export Images from Software Management (SWIM) Repository

These functions are only accessible to the Network Administrator, Network Operator and super users who have all of the roles.

If you do not have permission to run custom commands, you can run a command or command set from the CLI only if:

- The command set is assigned to you by the Administrator.
- The command set has at least one command that can be run on the specified device.

This section contains:

Running cwcli swim Command

The command syntax for running **`cwcli swim`** commands is:

`cwcli swim` *`subcommands common_arguments command_arguments`*

In the CLI version, you can provide the arguments in the (operating system shell) command line or in aninput file.

The input file gives you flexibility and control over commands and command sets. You can specify the images on which you want to run the command sets.

In the input file, you can include subcommands and command arguments.

Items in square brackets ([]) are optional; items in curly brackets ({}) are required.

The arguments are described in the following sections.

Subcommands

Subcommands specify the actions that you perform. Valid values for subcommands are described in the following table.

Sub Command	Description	Example
`listimages`	Displays a list of images available in the Software Repository.	`cwcli swim listimages -u` *Userid* `-p` *Password*
`exportimages`	Exports specified images in a non-compressed format from the Software Repository to any directory. The default target directory is the current directory. For exportimages command either one of these arguments is mandatory: `-imagenames`|`-all`|`-input`	`cwcli swim exportimages -u` *Username* `-p` *Password* [`-imagenames` *imagename1, imagename2...*] [`-all`] [`-dirname` *directoryname*] [`-input` *argumentFile*] [`-m` *email*][`-l` *logfile*]
`help`	Displays command usage information.	`cwcli swim -help`

Common Arguments

Common arguments specify parameters that apply to all subcommands. Valid values for*common_arguments* are described in the following table.

Command Arguments	Description/Action	Usage Notes
`-u` *user*	Enter a valid LMS username.	None
`-p` *password*	Enter the password for the username. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.	None
[`-l` *log_filename*]	Identifies a file to which Software Management Commands will write log messages. If you do not specify this, the log output will appear on screen.	This argument is optional. *log_filename* can be a full path to the file or a filename in the local directory. If you do not specify filename, the log file will be created in: • /var/adm/CSCOpx/log (On Solaris and Soft Appliance) • *NMSROOT*\log (On Windows) *NMSROOT* is the LMS install directory.
[`-m` *Email ID*]	Enter your Email ID	This argument is optional. You will get the output of the CLI operation in an e-mail.

Command Arguments

Command arguments specify parameters that apply only to specific subcommands. Valid values for command arguments are described in the following table.

Arguments in square brackets ([]) are optional. Arguments in curly brackets ({}) are required. You must provide one argument from each group of arguments in curly brackets ({}) that is separated by vertical bars (|).

Command Arguments	Description	Usage Notes
Command Arguments for `exportimages`		
{**`-imagenames`** *ImageName1, ImageName2*}	Specify the image names that you want to export using this command.	**`cwcli swim exportimages -u`** *Username* **`-p`** *Password* [**`-imagenames`** *imagename1, imagename2...*] [**`-all`**] [**`-dirname`** *directoryname*] [**`-input`** *argumentFile*] [**`-m`** *email*][**`-l`** *logfile*] *ImageName1, ImageName2* —List of images. Separate these names by commas.
{**`-all`**}	Specify this option if you want to export all images from Software Repository to the current directory or any specified directory.	--
{**`-input`** *argumentFile*}	Input file containing the details of the subcommands	If you are specifying the input file, you need not specify the subcommands. For instance, if you are using sample.txt as the argumentFile for -input command, you have to provide the following command: **`cwcli swim exportimages -input`** *sample.txt* Example of sample.txt: **`-imagenames`** {*imagename1}*, [*imagename2...*] **`-imagenames`** {*imagename4}*, [*imagename5...*] Items in square brackets ([]) are optional; items in curly brackets ({}) are required.
[**`-dirname`** *directoryname*]	Specify a directory name if you want to export images to a specified directory using this command.	If you do not specify this the images are exported to the NMSROOT/temp directory, where CLI is launched.

Running SWIM CLI Remotely

You can run Software Management (SWIM) CLI from a remote console.

SWIM uses the Remote Access feature in the CLI framework to help you to invoke the SWIM commands from the client in the same way as you run them on the LMS server.

The name of the servlet to be invoked is /rme/cwcli.

You must invoke the following URLs to run any command.

- For POST request:

  http://*lms-server:lms-port*/rme/**cwcli** *payload XML file*

- For GET request:

  http://*lms-server:lms-port*/rme/cwcli?command=**cwcli swim** *command* **-u** *Username* **-p** *Password command_specific_args*

The contents of the payload.xml is:

```
<payload>
<command>
cwcli swim command -u Username -p Password command_specific_args
</command>
</payload>
```

For example to execute the **listimages** command payload.xml will be as follows:

```
<payload>
<command>
cwcli swim listimages -u Username -p Password
</command>
</payload>
```

Note The *Base64* encoded password is used for accessing Software Management (SWIM) CLI remotely.

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

APPENDIX A

Config Template XML Schema

Cisco Prime LMS allows you to create new configuration templates (.xml format) that can be deployed using the Template Center feature.

This section explains:

- Understanding the XML Schema
- Sample Template for Identity - Change of Authorization

Understanding the XML Schema

This section explains the XML schema that you can use to create new templates (.xml format) and deploy them in LMS. See Detailed Description of Template XML Schema for more information.

The XML schema file is:

```
<xs:schema
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:jaxb="http://java.sun.com/xml/ns/jaxb"
      xmlns:xjc="http://java.sun.com/xml/ns/jaxb/xjc"
      jaxb:extensionBindingPrefixes="xjc"
    jaxb:version="1.0">


    <xs:annotation>
       <xs:appinfo>
          <jaxb:globalBindings generateIsSetMethod="true">
              <xjc:serializable uid="1255591397484"/><!--  14-Oct-2009  -->
          </jaxb:globalBindings>
       </xs:appinfo>
    </xs:annotation>


    <!--  Defining root OOTB template -->

    <xs:element name="ootb-template">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="template-metadata" type="template-metadata" minOccurs="1"
maxOccurs="1" />
                <xs:element name="config" type="config" minOccurs="1" maxOccurs="unbounded"
/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
```

```
    <!--  Defining the template meta data -->
    <xs:complexType name="template-metadata">
        <xs:all>
            <xs:element name="template-details" type="template-details"minOccurs="1"
maxOccurs="1" />
            <xs:element name="parameter-metadata" type="parameter-metadata" minOccurs="0"
maxOccurs="1" />
        </xs:all>
        <xs:attribute name="name" type="xs:string" use="required"/>
    </xs:complexType>

    <!-- Defining the template details -->
    <xs:complexType name="template-details">
        <xs:all>
            <xs:element name="description" type="xs:string" maxOccurs="1" minOccurs="1" />
            <xs:element name="task" type="xs:string" maxOccurs="1" minOccurs="0"/>
            <xs:element name="author" type="xs:string" maxOccurs="1" minOccurs="0"
default="Cisco Systems"/>
            <xs:element name="template-version" type="xs:string" maxOccurs="1"
minOccurs="0" />
            <xs:element name="scope" type="xs:string" default="Device" maxOccurs="1"
minOccurs="0" />
            <xs:element name="type" type="xs:string" default="Partial" maxOccurs="1"
minOccurs="0" />
            <xs:element name="features" type="xs:string" minOccurs="0" maxOccurs="1" />
            <xs:element name="pin" type="xs:string" minOccurs="0" maxOccurs="1" />
            <xs:element name="hardware-platform" type="xs:string" minOccurs="0"
maxOccurs="1" />
            <xs:element name="imagefeature" type="xs:string" minOccurs="0" maxOccurs="1"
/>
            <xs:element name="conflictingtag" type="conflictingtag" maxOccurs="1"
minOccurs="0" />
        </xs:all>
    </xs:complexType>


    <!--  Defining the conflicting tag details -->
    <xs:complexType name="conflictingtag">
    <xs:sequence>
        <xs:element name="platform" type="conflict-platform" minOccurs="1"
maxOccurs="unbounded" />
    </xs:sequence>
    </xs:complexType>

    <xs:complexType name="conflict-platform">
    <xs:sequence>
        <xs:element name="feature" type="featureType" maxOccurs="unbounded" minOccurs="1"
/>
    </xs:sequence>
    <xs:attribute name="name" type="xs:string" use="required" />

    </xs:complexType>

    <xs:complexType name="featureType">
    <xs:sequence>
        <xs:element name="cli-command" type="cli-command" minOccurs="0" maxOccurs="1" />
    </xs:sequence>

    <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
    <xs:attribute name="message" type="xs:string" use="required"></xs:attribute>
    </xs:complexType>

    <!-- Defining parameter meta data -->
```

```
    <xs:complexType name="parameter-metadata">
    <xs:sequence>
        <xs:element name="param-group" type="param-group"minOccurs="1"
maxOccurs="unbounded" />
    </xs:sequence>
    </xs:complexType>

    <xs:complexType name="param-group">
    <xs:sequence>
        <xs:element name="description" type="xs:string" maxOccurs="1" minOccurs="1" />
        <xs:element name="parameter" type="parameter"minOccurs="1" maxOccurs="unbounded"
/>
    </xs:sequence>
    <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
    <xs:attribute name="cliName" type="xs:string" use="required"></xs:attribute>
    <xs:attribute name="isMandatory" type="xs:boolean" use="required"></xs:attribute>
    </xs:complexType>

    <xs:complexType name="parameter">
    <xs:sequence>
        <xs:element name="description" type="xs:string"minOccurs="1" maxOccurs="1" />
            <xs:element name="html-component" type="xs:string"minOccurs="0" maxOccurs="1"
/>
            <xs:element name="default-value" minOccurs="0" maxOccurs="unbounded" >
                <xs:complexType>
                    <xs:simpleContent>
                        <xs:extension base="xs:string">
                            <xs:attribute name="label" type="xs:string"
use="optional"></xs:attribute>
                        </xs:extension>
                    </xs:simpleContent>
                </xs:complexType>
            </xs:element>
            <xs:element name="data-type" type="xs:string"minOccurs="0" maxOccurs="1" />
            <xs:element name="mandatory" type="xs:boolean"minOccurs="0" maxOccurs="1" />
             <xs:element name="isGlobal" type="xs:boolean"minOccurs="0" maxOccurs="1" />
             <xs:element name="help-description" type="xs:string"minOccurs="0"
maxOccurs="1" />
             <xs:element name="syntax" type="syntax"minOccurs="0" maxOccurs="1" />
        </xs:sequence>
    <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
    </xs:complexType>

    <xs:complexType name="syntax">
        <xs:all>
             <xs:element name="min" type="xs:string" minOccurs="0" maxOccurs="1" />
             <xs:element name="max" type="xs:string" minOccurs="0" maxOccurs="1" />
         <xs:element name="pattern" type="cli-command" minOccurs="0" maxOccurs="1" />
        </xs:all>
    </xs:complexType>



    <!-- Configuration details -->
    <xs:complexType name="config">
        <xs:sequence>
             <xs:element name="device-filtering-details" type="device-filtering-details" />
             <xs:element name="cli" type="cliType" minOccurs="0" maxOccurs="unbounded" />
        </xs:sequence>
        <xs:attribute name="platform" type="xs:string" use="required"/>
    </xs:complexType>

    <xs:complexType name="cliType">
        <xs:sequence>
```

```
            <xs:element name="clicommand" type="cli-command" minOccurs="1"
maxOccurs="unbounded" />
        </xs:sequence>
        <xs:attribute name="name" type="xs:string" use="required"/>
    </xs:complexType>

    <!-- Device filtering details -->

    <xs:complexType name="device-filtering-details">
        <xs:sequence>
        <xs:element name="family" type="family" minOccurs="1" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="family">
        <xs:all>
            <xs:element name="min-supported-imageversion"
type="min-supported-imageversion" minOccurs="1" maxOccurs="1" />
        </xs:all>
        <xs:attribute name="value" type="xs:string" use="required" />
    </xs:complexType>

    <xs:complexType name="min-supported-imageversion">
        <xs:sequence>
            <xs:element name="device-type" type="device-type" minOccurs="1"
maxOccurs="unbounded" />
        </xs:sequence>
        <xs:attribute name="value" type="xs:string" use="required" />
    </xs:complexType>

    <xs:complexType name="device-type">
        <xs:all>
            <xs:element name="name" type="xs:string" minOccurs="0" maxOccurs="1" />
            <xs:element name="sysobjectid" type="xs:string" minOccurs="0" maxOccurs="1" />
        </xs:all>
    </xs:complexType>


    <!--  configuration cli -->

    <xs:simpleType name="cli-command">
        <xs:restriction base="xs:string">
            <xs:annotation>
                <xs:appinfo>
                    <jaxb type="CDATA" />
                </xs:appinfo>
            </xs:annotation>
        </xs:restriction>
    </xs:simpleType>

</xs:schema>
```

Detailed Description of Template XML Schema

The table below describes elements in the XML schema.

Table A-1 Elements in the XML Schema

Xml Tag Name	Tag Description	Occurrence		Sample values
		Minimum	Maximum	
<ootb-template>	Any Template should start with this	1	1	<ootb-template> </ootb-template>
<template-metadata>	Configuration specific metadata should be under this tag. It has the following attribute: • name—Specifies the name of the Template. This name is used for identifying the template.	1	1	<template-metadata name="3750 access config">
<template-details>	This tag comes under template-metadata tag. This tag will take up the metadata such as description, task, author, revision to the template, date of the template creation	1	1	<template-details> </template-details>
<description>	This tag comes under template-details tag. Gives a small description about the template.	1	1	<description>c3750 stacked configuration</description>
<task>	This tag comes under template-details tag. It gives the functionality of the tag.	0	1	<task>Snmp Community settings</task>
<author>	This tag comes under template-details tag. It gives the name of the person who has created the template. Multiple names can be given separated by commas. By default, the author name is Cisco Systems.	0	1	<author>cisco systems</author>
<template-version>	This tag comes under template-details tag. It gives the revision number to the template.	0	1	<template-version>1.0</template-version>

Table A-1 Elements in the XML Schema

Xml Tag Name	Tag Description	Occurrence		Sample values
<scope>	This tag comes under template-details tag. It gives the scope of the template that accepts values of either Device, Port, Module	0	1	<scope>port</scope>
<type>	This tag comes under template-details tag. It refers to the type of the template taking values of either partial or complete.	0	1	<type>partial</type>
<features>	This tag comes under template-details tag. It gives the list of features for which this config can be applied. Features can be given in a comma separated values	0	1	<features>dhcp snoop, auto qos</features>
<pin>	This tag comes under template-details tag. It gives the devices in the network to which the template is applicable. Comma separated values are allowed	0	1	<pin>edge</pin>
<hardware-platform>	This tag comes under template-details tag. It gives the hardware type to which the template is applicable. Comma separated values are allowed.	0	1	<hardware-platform>stack</hardware-platform>
<imagefeature>	This tag comes under template-details tag. It gives the image feature that is required to apply this template.	0	1	<imagefeature>ipbase</imagefeature>
<conflictingtag>	This tag comes under template-details tag. The template cannot be applied when any cli is given under this tag.	0	1	<conflictingtag></conflictingtag>

Table A-1 Elements in the XML Schema

Xml Tag Name	Tag Description	Occurrence		Sample values
<platform>	This tag comes under conflictingtag tag. It has an attribute `name` that specifies to which platform the conflicting tag belongs to. Following are the values taken by name attribute: ios,catos,pixos,nam,Soft Appliance,ios_ssl,ios_wlsm,ios_mwam,ios_webvpn,webns,ACE, ACNS,CSM	1	Unlimited	<platform name="ios"> </platform>
<feature>	This tag will come under conflictingtag. It has the following attributes, • name—Name of the feature that is conflicting to this template. • message—Warning message that needs to be shown when this feature is available. • platform—Software platform to which this feature is conflicting to this template.	1	Unlimited	<feature name="dot1x" message="since dot1x conflict is there, do not configure the following template in the device." platform="ios"> </feature>
<cli-command>	This tag comes under feature tag. Cli which needs to be searched in a running configuration. If this configuration is found, the cli will not be deployed.	0	1	<cli-command>no aaa new-model clock summer-time utc recurring</cli-command>
<parameter-metadata>	This tag comes under template-metadata tag. This section describes the variables that are used in the template.	1	1	<parameter-metadata> </parameter-metadata>

Table A-1 Elements in the XML Schema

Xml Tag Name	Tag Description	Occurrence		Sample values
<param-group>	This tag comes under parameter-metadata tag and is used to group the parameters. For example, if there are five parameters, two can be grouped in one and the remaining three in another group. Attributes of this tag: • name—Name of the group • cliName—A key that maps the parameter group to a Cli group. Both cliName and the name of the cli should be same. • isMandatory—To indicate if this group is mandatory for the template or not. Useful in case of partial template, where you will have the option in the UI as Skip this section.	1	Unlimited	<param-group name="Identity Commands" cliName="identity" isMandatory="true" > </param-group>
<description>	This tag comes under param-group tag. Provides a simple description about the parameter. It is mandatory as this will be taken as a Label for the html component.	1	1	<description>Readonly Community String</description>
<parameter>	This tag comes under parameter-metadata tag. Describes about a single parameter to get input from the user. This parameter will be converted into a html component. Any variable defined in the cli should have a parameter tag defined. It takes the name as an attribute to this tag.	1	Unlimited	<parameter name="readonly">
<html-component>	This tag comes under parameter tag. Specifies what html component is rendered for the specified parmeter.	0	Unlimited	<html-component>textbox</html-component>

Table A-1 Elements in the XML Schema

Xml Tag Name	Tag Description	Occurrence		Sample values
<default-value>	This tag comes under parameter tag. Default value for the parameter. This tag can be used to give values for a select box. It has the following attribute: label—It is used to build the combo box content. The label value is displayed as a content to the combo box. The element value defined is considered as a selected value in the backend.	0	Unlimited	<default-value label="0-shut">0</default-value>
<data-type>	This tag comes under parameter tag. It specifies datatype of the input that is given to the parameter.	0	1	<datatype>integer</datatype> Boolean or Integer
<mandatory>	This tag comes under parameter tag. To specify if this parameter is mandatory parameter or not. Accepts value `true` or `false`.	0	1	<mandatory></mandatory>
<isGlobal>	This tag comes under parameter tag. To specify if this parameter is applicable for all devices or only one device. Accepts the following values: • true—applicable for all devices • false—applicable for per device level	0	1	<isGlobal></isGlobal>
<help-description>	This tag comes under parameter tag. Use for describing more about this parameter.	0	1	<help-description></help-description>
<syntax>	This tag come under parameter tag. To specify the validation part for numeric field and the string parameter.	0	1	<syntax></syntax>

Table A-1 Elements in the XML Schema

Xml Tag Name	Tag Description	Occurrence		Sample values
<min>	This tag comes under syntax tag. To specify the minimum value for a numeric field. The datatype should be numeric.	0	1	<Min>0</min>
<max>	This tag comes under syntax tag. To specify the maximum value for a numeric parameter. The datatype should be numeric.	0	1	<max>100</max>
<pattern>	This tag comes under syntax tag. To specify the regular expression for the string parameter. The requlars expression is used to validate the value that is specified by the user.	0	1	<patter>[a-z]*</pattern>
<config>	This tag comes under ootb-template tag. The respective config which needs to be deployed into the devices is defined here. For example, config tag should come under OOTB-Template It has the following attribute: platform—Specifies to what software platform this config is applicable. Following are the values taken by this attribute: ios,catos,pixos,nam,Soft Appliance,ios_ssl,ios_wlsm,ios_mwam,ios_webvpn,webns,ACE, ACNS,CSM	1	1	<config></config>
<device-filtering-details>	This tag comes under config tag. To specify the filtering details for the device.	1	1	<device-filtering-details></device-filtering-details>
<family>	This tag comes under device-filtering-details tag. To specify what family this filtering belongs to. The Value should be as specified in mdfData.xml for the supported devices.	1	Unlimited	<family value="cisco catalyst 3750-e series switches"> </family>

Table A-1 Elements in the XML Schema

Xml Tag Name	Tag Description	Occurrence		Sample values
<min-supported-image version>	This tag come under family tag. To specify the minimum supported image version to which this template will be applicable.	1	1	<min-support-imageversion>12.2(40)se</min-support-imageversion>
<device-type>	This tag comes under min-supported-imageversion. To specify which device type this template will be applicable.	1	Unlimited	<device-type> </device-type>
<name>	This tag comes under device-type tag. It gives the MDF name of the device type.	0	1	<name> </name>
<sysobjectid>	This tag comes under device-type tag. It gives the sysobjectid of the device.	0	1	<sysObjectId></sysObjectId>
<cli>	This tag come under config tag. It specifies the cli for the mentioned software platform. It has the attribute called `name`. The value should be same as that of param-group name. This is used to map the param-group to that of cli.	0	Unlimited	<cli name="snmpSecurity">
<clicommand>	This tag comes under cli tag. To specify the command that will be deployed.	1	Unlimited	<clicommand><![CDATA[]]></clicommand>
<MLTCMD>	To specify multi-line commands like, banner and crypto certificate commands. The commands within the MLTCMD tags are considered as a single command and will be downloaded as a single command onto the device These tags are case-sensitive and you must enter them only in uppercase. You cannot start this tag with a space. You can have a blank line within a multi-line command.	0	Unlimited	If you use this tag between cdata tags, then you must use <MLTCMD>. For example: <MLTCMD>banner login "Welcome to Cisco Prime LMS - you are using Multi-line commands" </MLTCMD> If cdata is not present, then you must use <MLTCMD>. For example: <MLTCMD> banner login "Welcome to Cisco Prime LMS - you are using Multi-line commands" </MLTCMD>

Sample Template for Identity - Change of Authorization

The section shows the template for Identity - Change of Authorization:

```
<?xml version="1.0"
encoding="iso-8859-1"?><!--*****************************************************-->
<!--         Copyright (c) 2009, 2010 Cisco Systems, Inc.     -->
<!--         All rights reserved.                          -->
<!--*****************************************************-->


<ootb-template>
<template-metadata name="Identity - Change of Authorization">
        <template-details>
                 <description>Identity - Change of Authorization</description>
                 <task>Identity</task>
                 <author>Cisco Systems</author>
                 <template-version>1.0</template-version>
                 <scope>Device</scope>
                <type>partial</type>
                 <features></features>
                 <pin>edge</pin>
                 <hardware-platform>Device</hardware-platform>
                <imagefeature>ipbase</imagefeature>
         </template-details>
         <parameter-metadata>
        <param-group name="Identity Commands" cliName="identity" isMandatory="true" >
        <description>A standard RADIUS interface is one where the request for
authorization originates from the device attached to the network, and the response comes
from the queried RADIUS servers. However, Catalyst Switches support the RADIUS Change of
Authorization (CoA). CoA allows for the dynamic reconfiguration of sessions from external
RADIUS servers.</description>
    <parameter name="ipaddress">
    <description>RADIUS client IP address or Host name</description>
    <html-component>textbox</html-component>
    <default-value></default-value>
    <data-type>string</data-type>
    <mandatory>true</mandatory>
    <isGlobal>true</isGlobal>
    <help-description></help-description>
    <syntax>
        <min></min>
        <max></max>
        <pattern></pattern>
    </syntax>
</parameter>
<parameter name="authtype">
    <description>Type of authorization the device uses for RADIUS clients</description>
    <html-component>select</html-component>
    <default-value label="any">any</default-value>
    <default-value label="all">all</default-value>
    <default-value label="session-key">session-key</default-value>
    <data-type>string</data-type>
    <mandatory>true</mandatory>
    <isGlobal>true</isGlobal>
    <help-description></help-description>
    <syntax>
            <min></min>
            <max></max>
            <pattern></pattern>
    </syntax>
```

```
</parameter>

<parameter name="server-key">
    <description>RADIUS Key shared between the device and RADIUS clients</description>
    <html-component>password</html-component>
    <default-value></default-value>
    <data-type>string</data-type>
    <mandatory>true</mandatory>
    <isGlobal>true</isGlobal>
    <help-description></help-description>
    <syntax>
            <min></min>
            <max></max>
            <pattern></pattern>
    </syntax>
</parameter>

<parameter name="port">
    <description>Port on which the device listens for RADIUS requests [0 -
65535]</description>
    <html-component>textbox</html-component>
    <default-value>1700</default-value>
    <data-type>numeric</data-type>
    <mandatory>true</mandatory>
    <isGlobal>true</isGlobal>
    <help-description></help-description>
    <syntax>
            <min>0</min>
            <max>65535</max>
            <pattern></pattern>
    </syntax>
</parameter>
</param-group>

</parameter-metadata>
</template-metadata>
<config platform="ios">
 <device-filtering-details>
       <family value="Switches and Hubs">
           <min-supported-imageversion value ="12.2(52)SE">
              <device-type>
                 <name>Cisco Catalyst 2960-24TC Switch</name>
                 <sysobjectid>1.3.6.1.4.1.9.1.694</sysobjectid>
              </device-type>
              <device-type>
                 <name>Cisco Catalyst 2960-48TC Switch</name>
                 <sysobjectid>1.3.6.1.4.1.9.1.695</sysobjectid>
              </device-type>
              <device-type>
                 <name>Cisco Catalyst 2960G-24TC Switch</name>
                 <sysobjectid>1.3.6.1.4.1.9.1.696</sysobjectid>
              </device-type>
              <device-type>
                 <name>Cisco Catalyst 2960G-48TC Switch</name>
                 <sysobjectid>1.3.6.1.4.1.9.1.697</sysobjectid>
              </device-type>
              <device-type>
                 <name>Cisco Catalyst 2960-24TT Switch</name>
                 <sysobjectid>1.3.6.1.4.1.9.1.716</sysobjectid>
              </device-type>
              <device-type>
                 <name>Cisco Catalyst 2960-48TT Switch</name>
                 <sysobjectid>1.3.6.1.4.1.9.1.717</sysobjectid>
              </device-type>
```

```
<device-type>
   <name>Cisco Catalyst 2960-8TC Compact Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.798</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960G-8TC Compact Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.799</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-24-S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.929</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-24TC-S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.928</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-48TC-S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.927</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-24PC-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.950</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-24LT-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.951</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960PD-8TT-L Compact Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.952</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-8TC-S Compact Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1006</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-48TT-S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1005</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-48PST-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1016</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-24LC-S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1146</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-24PC-S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1147</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960-48PST-S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1148</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Enhanced Layer 2 EtherSwitch Service Module</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1048</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Enhanced Layer 2 EtherSwitch Service Module</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1051</sysobjectid>
</device-type>
```

```
<device-type>
   <name>Cisco Enhanced Layer 2 EtherSwitch Service Module</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1052</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Enhanced Layer 2 EtherSwitch Service Module</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1055</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-48TS-S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1256</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-24TS-S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1257</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-48FPD-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1258</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-48LPD-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1259</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-48TD-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1260</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-24PD-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1261</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-24TD-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1262</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-48FPS-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1263</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-48LPS-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1264</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-24PS-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1265</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-48TS-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1266</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960S-24TS-L Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1267</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2960 stack</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1208</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 2926 Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.5.35</sysobjectid>
</device-type>
```

```
            <device-type>
               <name>Cisco Catalyst 2980G-A Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.5.51</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 2980G-A Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.5.49</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 2948G-GE-TX Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.5.62</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 2975 Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.1068</sysobjectid>
            </device-type>
         </min-supported-imageversion>
      </family>

      <family value="Switches and Hubs">
         <min-supported-imageversion value ="12.2(52)SE">
            <device-type>
               <name>Cisco Catalyst 3560G-24PS Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.614</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 3560G-24TS Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.615</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 3560G-48PS Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.616</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 3560G-48TS Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.617</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 3560 Series Switches</name>
               <sysobjectid>1.3.6.1.4.1.9.1.563</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 3560-48PS Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.564</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 3560-24TS Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.633</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 3560-48TS Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.634</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 3560E-24TD-E,S Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.793</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 3560E-48TD-E,S Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.794</sysobjectid>
            </device-type>
            <device-type>
               <name>Cisco Catalyst 3560E-24PD-E,S Switch</name>
               <sysobjectid>1.3.6.1.4.1.9.1.795</sysobjectid>
```

```
</device-type>
<device-type>
   <name>Cisco Catalyst 3560E-48PD-E,S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.796</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3560-8PC Compact Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.797</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3560E-12D-S,E Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.930</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3560E-12SD-E,S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.956</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3560-12PC-S Compact Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1015</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3560V2-48PS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1025</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3560V2-24DC Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1019</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3560V2-24TS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1020</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3560V2-24PS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1021</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3560V2-48TS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1024</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1049</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1050</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1053</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1054</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1056</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Enhanced Layer2,Layer3 EtherSwitch Service Module</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1057</sysobjectid>
```

```
                </device-type>
                <device-type>
                   <name>Cisco Catalyst 3560X-24T-L,S Switch</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.1226</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco Catalyst 3560X-48T-L,S Switch</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.1227</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco Catalyst 3560X-24P-L,S Switch</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.1228</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco Catalyst 3560X-48PF-L,S Switch</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.1229</sysobjectid>
                </device-type>
             </min-supported-imageversion>
          </family>

          <!-- Cisco Catalyst 3750 Series Switches and Similar categories -->
          <family value="Switches and Hubs">
             <min-supported-imageversion value ="12.2(52)SE">
                <device-type>
                   <name>Cisco 3750 Stack</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.516</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco Catalyst 3750G-12S Switch</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.530</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco Catalyst 3750-24PS Switch</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.536</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco 2600,2800,3700,3800 Series 16-Port EtherSwitch Service
Module</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.663</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco 2800,3800 Series 23-Port EtherSwitch Service Module</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.664</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco 2851,3800 Series 48-Port EtherSwitch Service Module</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.666</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco 2851,3800 Series 24-Port EtherSwitch (with Stackwise
Connectors) Service Module</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.665</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco 2600,2800,3700,3800 Series 16-Port EtherSwitch Service
Module</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.702</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco Catalyst 3750 Metro 24-DC Switch</name>
                   <sysobjectid>1.3.6.1.4.1.9.1.574</sysobjectid>
                </device-type>
                <device-type>
                   <name>Cisco Catalyst 3750G-12S-SD Switch</name>
```

```
   <sysobjectid>1.3.6.1.4.1.9.1.688</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750E-24TD-E,S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.789</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750E-48TD-E,S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.790</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750E-48PD-E,S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.791</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750E-24PD-E,S Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.792</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750G-24 Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.511</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750G-48 Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.512</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750-24TS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.513</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750G-24T Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.514</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750-48PS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.535</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750G-24PS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.602</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750G-48PS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.603</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750G-48TS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.604</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750G-24TS-1U Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.624</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750-24FS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.656</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750V2-48PS Switch</name>
   <sysobjectid>1.3.6.1.4.1.9.1.1027</sysobjectid>
</device-type>
<device-type>
   <name>Cisco Catalyst 3750V2-24PS Switch</name>
```

```
            <sysobjectid>1.3.6.1.4.1.9.1.1023</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 3750V2-24TS Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.1022</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 3750V2-48TS Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.1026</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 3750X-24T-L,S Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.1222</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 3750X-48T-L,S Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.1223</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 3750X-24P-L,S Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.1224</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 3750X-48PF-L,S Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.1225</sysobjectid>
         </device-type>
      </min-supported-imageversion>
   </family>

   <family value="Switches and Hubs">
      <min-supported-imageversion value ="12.2(50)SG">
         <device-type>
            <name>Cisco Catalyst 4503 Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.5.58</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 4506 Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.5.59</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 4506-E Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.875</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 4510R-E Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.877</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 4503-E Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.874</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 4507R-E Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.876</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 4507R Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.501</sysobjectid>
         </device-type>
         <device-type>
            <name>Cisco Catalyst 4506 Switch</name>
            <sysobjectid>1.3.6.1.4.1.9.1.502</sysobjectid>
         </device-type>
         <device-type>
```

```
                    <name>Cisco Catalyst 4503 Switch</name>
                    <sysobjectid>1.3.6.1.4.1.9.1.503</sysobjectid>
                </device-type>
                <device-type>
                    <name>Cisco Catalyst 4510R Switch</name>
                    <sysobjectid>1.3.6.1.4.1.9.1.537</sysobjectid>
                </device-type>
            </min-supported-imageversion>
        </family>

        <!-- Cisco Catalyst 6500 Series Switches and Similar categories -->
        <family value="Switches and Hubs">
           <min-supported-imageversion value ="12.2(33)SXI">
            <device-type>
                <name>Cisco Catalyst 6513 Switch</name>
                <sysobjectid>1.3.6.1.4.1.9.1.400</sysobjectid>
            </device-type>
            <device-type>
                <name>Cisco Catalyst 6509-NEB-A Switch</name>
                <sysobjectid>1.3.6.1.4.1.9.1.534</sysobjectid>
            </device-type>
            <device-type>
                <name>Cisco Catalyst 6506 Switch</name>
                <sysobjectid>1.3.6.1.4.1.9.1.282</sysobjectid>
            </device-type>
            <device-type>
                <name>Cisco Catalyst 6509-NEB Switch</name>
                <sysobjectid>1.3.6.1.4.1.9.1.310</sysobjectid>
            </device-type>
            <device-type>
                <name>Cisco Catalyst 6509 Switch</name>
                <sysobjectid>1.3.6.1.4.1.9.1.283</sysobjectid>
            </device-type>
            <device-type>
                <name>Cisco Catalyst 6504-E Switch</name>
                <sysobjectid>1.3.6.1.4.1.9.1.657</sysobjectid>
            </device-type>
            <device-type>
                <name>Cisco Catalyst 6509-V-E Switch</name>
                <sysobjectid>1.3.6.1.4.1.9.1.832</sysobjectid>
            </device-type>
            <device-type>
                <name>Cisco Catalyst 6500 Series SSL Services Module</name>
                <sysobjectid>1.3.6.1.4.1.9.1.554</sysobjectid>
            </device-type>
            <device-type>
                <name>Cisco Catalyst 6503 Switch</name>
                <sysobjectid>1.3.6.1.4.1.9.1.449</sysobjectid>
            </device-type>
           </min-supported-imageversion>
        </family>
</device-filtering-details>
    <cli name="identity">
    <clicommand>
        <![CDATA[
            aaa server radius dynamic-author
            client ${ipaddress}
            server-key ${server-key}
            port ${port}
            auth-type ${authtype}
        ]]>
    </clicommand>
</cli>
</config>
```

```
</ootb-template>
```

APPENDIX B

Troubleshooting Tips and FAQs

This appendix covers the Troubleshooting tips and FAQs for:

- Configuration Archive
- NetConfig
- Config Editor
- Software Management
- Job Approval
- cwcli config
- cwcli export
- VRF Lite

For Installation related FAQs and Troubleshooting tips, see the *Installing and Migrating to CiscoWorks LAN Management Solution 4.1*.

Configuration Archive

This section provides the troubleshooting information and FAQs for Configuration Archive:

- Configuration Archive FAQs
- Troubleshooting Configuration Archive

This section contains:

- Login Authentication in Telnet Mode
- Login Authentication in SSH Mode
- Enable Login Authentication in Telnet Mode
- Enable Login Authentication in SSH Mode

Configuration Archive FAQs

Q. Can I define the protocol order for configuration fetch and deploy?

A. Yes, you can define the order of protocol that has to be used for Configuration Management applications (Configuration Archive, Config Editor, and NetConfig). You can define this in the Transport Settings window (**Admin > Collection Settings > Config > Config Transport Settings**).

Q. When I select:

a. TFTP alone as the configuration transport protocol

b. Run Sync Archive Job for a device

c. Run a data capture trace

The data capture trace shows Telnet traffic along with SNMP/TFTP sessions.

Why does the Telnet session appear in the data capture trace although I have selected TFTP as the configuration transport protocol?

Q. The Telnet session that appears in the data capture trace is a socket connection to the Telnet port. It identifies the IP address of the CiscoWorks LMS server. This is important in multi-homed servers where the IP address that CiscoWorks server uses to contact the device, has to be identified.

Q. How Configuration Management interprets device credentials?

A. You can enter the device credentials when you,

- Add/import devices using the LMS Device Management option (**Inventory > Device Administration > Add / Import / Manage Devices**). In this flow, you can enter:
  - Primary Username—User name for the device.
  - Primary Password—Password for the device.
  - Primary Enable Password—Console-enabled password for the device.
- If you have enabled Enable Job Password option (**Admin > Network > Configuration Job Settings > Config Job Policies)** then while scheduling for a job, you can enter these credentials:
  - Login User name—User name for the device.
  - Login Password—Password for the device.
  - Enable Password—Console-enabled password for the device.

  These credentials are used while running the job. The credentials that you have entered in the Device and Credential Repository are ignored while running the job.

TACACS (Terminal Access Controller Access Control System) uses a separate centralized server to track usernames and passwords. This simplifies authentication and authorization, because information is maintained in only one database rather than being spread out over many devices.

If your devices are configured to use TACACS, you must provide TACACS device credentials when you add or import the devices.

Login Authentication in Telnet Mode

When LMS logs into non-privileged mode (User mode), depending on your device authentication configuration, the device will prompt for either username and password, or password only.

If the device prompts for username and password, LMS responds with the following:

- If Primary Username and Primary Password credentials are entered in the Device and Credential Repository, LMS sends Primary Username and Primary Password to the device.

  If you have enabled Enable Job Password option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (**Inventory > Device Administration > Add / Import / Manage Devices**) is ignored.

- If:
  - Authentication fails with the Primary credentials or Login User name and Login Password

    Or
  - The Primary credentials or Login User name and Login Password are not present in the database.

  LMS reports the login as failure.

If the device prompts for password only, LMS responds with the following:

- If Primary Password is entered in the database, LMS sends Primary Password to the device.

  If you have enabled Enable Job Password option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (**Inventory > Device Administration > Add / Import / Manage Devices**) is ignored.

  If you have configured only the Telnet password (without configuring username) on your device. You have to enter a string in the Login Username field. That is, you cannot leave the Login Username field blank.

  The Login Username string will be ignored while connecting to the device as the device is configured only for the Telnet password.

- If:
  - Authentication fails with the Primary Password or Login Password

    Or
  - The Primary Password or Login Password is not present in the database.

  LMS reports the login as failure.

Login Authentication in SSH Mode

This section describes how the device credentials are interpreted by LMS in SSH mode.

Open an SSH session to the device.

The device prompts for username and password, LMS responds with the following:

- If Primary Username and Primary Password are entered in the database, LMS sends Primary Username and Primary Password to the device.

If you have enabled Enable Job Password option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (**Inventory > Device Administration > Add / Import / Manage Devices**) is ignored.

- If:
  - Authentication fails with the Primary credentials or Login User name and Login Password

    Or
  - The Primary credentials or Login User name and Login Password are not present in the database

    LMS reports the login as failure.

Enable Login Authentication in Telnet Mode

This section describes how the TACACS and other credentials are interpreted by LMS in Telnet mode.

Logging into the Privileged mode (Enable mode) involves two steps:

1. LMS logs into non-privileged mode (See Login Authentication in Telnet Mode).
2. If logging into non-privileged mode is successful, LMS issues “enable” command for the device to enter into privileged mode.

   If the device prompts for password, LMS responds with the following:
   - If Primary Enable password is entered in the database, LMS sends Enable Primary password to the device.

     If you have enabled Enable Job Password option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (**Inventory > Device Administration > Add / Import / Manage Devices**) is ignored..
   - If authentication fails or Enable Password or Primary Enable Password is not present in database

     or
   - If logging into non-privileged mode fails or authentication fails in all above cases.

     LMS reports the login as failure.

Enable Login Authentication in SSH Mode

This section describes how the TACACS and other credentials are interpreted by LMS in SSH mode.

Logging into the Privileged mode (Enable mode) involves two steps:

1. LMS logs into non-privileged mode (See Login Authentication in SSH Mode).
2. If logging into non-privileged mode is successful, LMS issues the **enable** command for the device to enter into privileged mode.

   If the device prompts for password, LMS responds with the following:
   - If Primary Enable Password is entered in the database, LMS sends Primary Enable password to the device.

If you have enabled Enable Job Password option in the Job Policy dialog box (**Admin > Network > Configuration Job Settings > Config Job Policies**) and if you have entered the Login Password at the time of scheduling a job, LMS sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (**Inventory > Device Administration > Add / Import / Manage Devices**) is ignored.

- If authentication fails or Enable Password or Primary Enable Password is not present in database

  or

- If logging into non-privileged mode fails or authentication fails in all above cases.

  LMS reports the login as failure.

Q. What are the supported device prompts?

A. The supported device prompts are:

The supported Device authentication prompts are:

- Routers

  “Username:”, “Username: ”

  “Password:”, “Password: ”

- Switches

  “username: ”, “Username: ”

  “password: ”, "Password: ”

- Cisco Interfaces and Modules — Network Analysis Modules

  “login: ”

  “Password: ” “password: ”

- Security and VPN — PIX

  “username: ”, “Username: ”

  “passwd: ”, “password: ”, “Password: ”

- Content Networking—Content Service Switch

  “Username: ”, “username: ”, “login: ”,“Username:” , “username:” , “login:”

  “Password: ”, “password: ”, “passwd: ”,”Password:” , “password:” , “passwd:”

- Content Networking — Content Engine

  “Username: ” ,”login: ”

  “Password: ”

- Storage Networking — MDS Devices

  “Username:”, “Username: ”

  “Password:”, “Password: ”

Troubleshooting Configuration Archive

Message ID	Error Message	Probable Cause	Possible Action
CM0003	Version $1 does not exist in archive $2	Version may have been deleted	None
CM0005	Archive does not exist for $1	Error during archive creation.	Check the file system/user privileges.
CM0006	Archives do not exist	Error during archive creation.	Check the file system/user privileges.
CM0008	Checkout not permitted on archive $1	You may not have the required permission	Check with the administrator for your privilege.
CM0010	Checkin not permitted on archive $1	You may not have the required permission	Check with the administrator for your privilege.
CM0011	Delete not permitted	You may not have the required permission	Check with the administrator for your privilege.
CM0012	Could not create new version on archive $1	Insufficient disk space or config file may be incomplete.	Check whether disk space is available and that the directory has required permissions
CM0013	Cannot delete version on archive $1	You may not have the required permission	Check with the administrator for your privilege.
CM0015	Could not check out config for archive $1	You may not have the required permission	Check with the administrator for your privilege.
CM0016	Could not undo check out config for archive $1	You may not have the required permission	Check with the administrator for your privilege.
CM0017	Could not check in config for archive $1	$2	Check whether the file system is full and if you have required permissions.
CM0021	Version does not exist in archive $1	Version may have been deleted	None
CM0022	Archive already exists	Archive names should be unique	Enter a different name
CM0023	Archive creation not permitted	You may not have the required permission	Check with the administrator for your privilege.
CM0024	Error while deleting archive	You may not have the required permission	Check with the administrator for your privilege.
CM0025	Cannot delete device archive	Only the system purge can delete the device archive	Schedule for a purge job.
CM0026	Archive Relocation failed	The destination folder may not have the required disk space or required permission.	• Check if the destination folder has the required permission • Check if the disk space is available • Check if the user has the write permission.
CM0034	Cannot list versions for $1	You may not have the required permission or version do not exist.	Check with the administrator for your privilege.
CM0037	Database Connection Error	Database Engine may be down	Restart the RMEDbMonitor and CmfDbMonitor services

Message ID	Error Message	Probable Cause	Possible Action
CM0038	Error in Database	Database Engine may be down	Restart the RMEDbMonitor and CmfDbMonitor services
CM0040	Error while reading the file from the system	Either: • The file may not exist Or • You may not have required permissions.	Verify whether you have the correct privileges and that the file system is not corrupted.
CM0041	Error while writing the file to the system	Either: • The file may not exist Or • You may not have required permissions.	Verify whether you have the correct privileges and that the file system is not full
CM0043	Error while copying the file	Either: • The source or destination file may not exist Or • You may not have required permissions.	Verify whether: • The files exist • The file system is not full. • You have permission
CM0050	Cannot compare the configurations since they are not of the same type.	Configuration types are different	Select device of the same type.
CM0051	Cannot connect to ConfigMgmtSever process	Process may be down or maximum connection have been reached.	Restart the ConfigMgmtSever process.
CM0054	Error while initializing Transport for $1	Device packages may not exist.	Check whether: • The user exists in LMS and has required permissions, • Device is reachable • Required device packages are available in LMS.
CM0076	Job creation failed	$1	Check whether Jrm and CTMJrmServer processes are running
CM0077	Job modification failed	$1	Check whether Jrm and CTMJrmServer processes are running
CM0080	Could not send e-mail.	The e-mail configuration in your profile may be either missing or incorrect	Check e-mail configuration.
CM0082	Job execution failed.	The job policy may not be enabled	Enable the policy and try again
CM0085	Cannot list jobs of type	Jobs of this type may not exist in LMS.	Enable the policy and try again.

Message ID	Error Message	Probable Cause	Possible Action
CM0086	Cannot load job with id.	Job may not exist in LMS	Verify that the Job ID exists and try again
CM0087	Cannot obtain lock on device	Another application/job may have locked the device.	Verify that there are no other jobs is running on the device. Retry the job after some time.
CM0088	Configuration archival failed for $1	Not enough disk space.	Check whether the device is reachable and that the credentials are correct.
CM0090	Reload task failed on device	Device many not be reachable.	Check whether the device is reachable and that the credentials are correct.
CM0096	Job ID is not valid	The job may not exist in LMS	Verify that the job exists and try again.
CM0097	No failed devices in the job	There may not be any failed devices in the job.	Check for failed devices and try again.
CM0098	Invalid Job-based password specified	The Job-based password data may be null or cannot be used.	Enter the correct Job-based password and try again.
CM0109	Cannot read admin preferences.	Application may not have been initialized correctly	Retry the task
CM0122	No commands to write.	Command may not be available	Verify whether there are any commands to deploy
CM0123	Exception while getting all baseline templates.	Templates may have been deleted	Check if the template exist.
CM0125	Cannot persist template.	Template may be empty or invalid.	Check whether the commands are valid
CM0126	Cannot find baseline archive $1	Archive may have been deleted	Check if the archive exist.
CM0128	Cannot get baseline branch.	Branch may not exist.	Check if the branch exist.
CM0131	Cannot find template	Template may have been deleted	Check if the template exist.
CM0132	Cannot find result for job	Job may not exist.	Check if the job has been deleted.
CM0133	Invalid check-type for command	Check type may be invalid	Verify if the check-type is valid.
CM0136	Regular expression match failed.	Not a valid Regular expression.	Check if the expression is valid.
CM0137	No commandlets.	None	None
CM0138	Cannot find result for device	Device has been deleted.	Check if the device exist.
CM0139	Could not archive configuration	File system may be full or user may not have the required permission.	Check whether device is reachable and device credentials are correct. Increase timeout value, if required.
CM0148	User or device authorization failed.	User may not exist or does not have privileges to operate on any or all of the devices in the job.	Check whether the user exists and has required privileges to execute jobs.
CM0201	Could not start the SdiEngine.	The package path may be incorrect	Check whether the specified package path is correct

Message ID	Error Message	Probable Cause	Possible Action
CM0202	Could not access the device using SNMP.	SNMP may be disabled on the device	Check the Read Community string
CM0203	Could not create the CIDS Device Representation for device	Device package may not exist	Check if the required device packages are installed.
CM0204	Could not create Device Context for the device	Device package may not exist	Check whether the required device packages are available in LMS.
CM0205	Device package not found	Device package may not exist	Check whether the required device packages are available in LMS.
CM0206	Could not get the configuration transport implementation for $1	Device package may not exist	Check whether the required device packages are available in LMS.
CM0207	Could not get configuration analyzer implementation for $1	Device package may not exist	Check whether the required device packages are available in LMS.
CM0210	Cannot generate processed configuration	Configuration file may be corrupted or incomplete	Check that device returns complete configuration and the configuration file is not empty.

NetConfig

This section provides the troubleshooting information and FAQs for NetConfig:

NetConfig FAQs

Q. What are the supported protocols for NetConfig Reload task?

A. The supported protocols for NetConfig Reload task are Telnet, SSH and TFTP.

SSH and TFTP protocols are supported by NetConfig Reload task only if these protocols are also supported by the devices.

Troubleshooting NetConfig

This section provides the troubleshooting information for the NetConfig application:

Message ID	Error Message	Probable Cause	Possible Action
CFG0025	Cannot retry.	Retry is not supported on periodic jobs.	None.
CFG0026	You can retry only failed jobs.	A Successful job has been selected instead of a Failed job.	Select a Failed job and try again.
CFG0029	Job approval is enabled.	You have scheduled a job that requires Job approval with the Immediate schedule type. The job will run only when it has been approved by the Approver.	Do not select Immediate job type while scheduling the job.
CFG0009	Error occured while processing.	Check netconfigclient.log for more details.	Retry the operation. If the problem persists, send the logs to Cisco Technical Assistance Center (TAC). The netconfig logs are available at this location: On Windows: *NMSROOT*\log\netconfigclient.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/netconfigclient.log
CFG0029	Job approval is enabled.	This job requires job approval. So it can run only when the job is approved. So you cannot schedule a job with immediate schedule type.	Do not select Immediate schedule type.
CFG0041	You have selected an instance that does not have a task associated with it.	None.	Select an instance that has an associated task.

Config Editor

This section provides the troubleshooting information for the Config Editor application:

Message-ID	Error Message	Probable Cause	Possible Action
CEDT0001	No device selected	You have not selected a device.	Select a device and try again.
CEDT0002	There is no configuration file for the device.	There is no configuration file for the selected device in the archive.	Perform Synch Archive to get the configuration file for the device
CEDT0003	Modified Config not selected.	You have not selected a modified configuration from the Modified Configs list.	Select a configuration file from Modified Configs list.
CEDT0004	No Config Selected for Download.	You have not selected a configuration file for downloading either from the archive or from Modified Configs list.	Select a configuration file for downloading either from the archive or the Modified Configs list.
CEDT0005	Enter job description.	You have not entered a job description while creating a job	Enter the job description. This is mandatory.
CEDT0007	No job selected.	You have not selected a job.	Select a job
CEDT0009	Job {JobId} cannot be {Action}.	You have tried to do any of the following: • Edit a completed job • Copy an incomplete job • Stop a completed job • Stop an already stopped job.	User should select the appropriate job and appropriate action.
CEDT0010	Cannot get details for Job {JobID}.	The Job was recorded incorrectly.	None.
CEDT0011	Could not get the summary of the job.	None.	Check Cfgedit.log for more details.
CEDT0012	Job not found.	None	Check Cfgedit.log for more details. Contact Cisco TAC with log details for further assistance.
CEDT0013	Some change in Jsp leading to incompatible with Action class.	None.	Check cfgedit.log for more details. Contact Cisco TAC with log details for further assistance.
CEDT0014	Label not selected for search	You have tried to search labeled configurations without selecting a label	Select a label from the drop down.
CEDT0015	Cannot open configuration file.	None.	Check Cfgedit.log for more details. Contact Cisco TAC with log details for further assistance.

Message-ID	Error Message	Probable Cause	Possible Action
CEDT0016	Cannot open Baseline Template.	Template may be deleted	Check whether the template exists.
CEDT0017	Baseline Templates not present for the selected device.	There are no templates for the selected device type.	Create a Baseline Template for the selected device type from the archive.
CEDT0018	No Config found for the specified search pattern	The pattern you have entered cannot be found in any of the configs	Change the search pattern.
CEDT0019	External Config to be opened not selected	You have not selected an External Config.	Select the External Config File from the browser.
CEDT0020	Invalid configuration file.	Configuration file is corrupted.	Recreate config.
CEDT0021	Version to be opened not selected.	None.	Select a valid version
CEDT0022	Cannot load query. Check whether the query exists.	The query you selected may have been deleted.	Use Configuration > Configuration Archive > Views > Custom Queries to check whether the query exists. Create a query if it does not exist.
CEDT0023	Cannot find query. Check whether the query exists	The query you selected may have been deleted.	Use Configuration > Configuration Archive > Views > Search Archive> to check whether the query exists. Create a query if it does not exist.
CEDT0024	No External Syntax Checker is registered with CMIC.	Either: • You may have launched the External Syntax checker without registering the syntax checker tool with CMIC. or • The syntax checker is not registered correctly with CMIC.	Register the syntax checker tool correctly with CMIC before Launching External Syntax checker.
CEDT0025	Syntax Checking functionality is not supported by this device image.	The device image you have selected does not support Syntax Checking functionality.	Select another device image that supports Syntax Checking functionality.
CEDT0029	One or more of the devices selected are already added to this job.	A config for the device has already been added	Only one config can be downloaded to a device in a Job.
CEDT0030	No configuration file exists for the device	There is no configuration file for the selected device in the archive.	Perform Synch Archive to get the configuration file for the device
CEDT0031	There are no commands to download.	None.	Remove the device from job and try again.

Message-ID	Error Message	Probable Cause	Possible Action
CEDT0032	Approval is enabled. Cannot schedule immediate jobs.	You cannot schedule Immediate jobs if Approval is enabled.	Select Schedule type, Once instead of Immediate
CEDT0033	Selected Job Execution date is invalid.	You have selected a past date for running a job.	Select a valid future date.
CEDIT0034	Job user name or password not entered.	You have enabled the Job based password option but not entered password.	Either: • Deselect the Job-based password option Or • Enter the user name and password fields.
CEDT0039	Enter at least one pattern.	You have not entered any search patterns.	Either: • Select one of the queries listed Or • Enter a search pattern.

Software Management

This section provides the troubleshooting information and FAQs for the Software Management applications:

- Software Management FAQs
- Troubleshooting Software Management

Software Management FAQs

- Q.What are the high-level features of Software Management?
- Q.What privilege level is required to run Software Management functions?
- Q.How do I know which functions I can access in Software Management?
- Q.Are there DNS dependencies for Remote Copy Protocol (RCP) to work properly for a device?
- Q.Can I use Remote Copy Protocol (RCP) to transfer images to devices?
- Q.What connection mechanism does Software Management use to upgrade software?
- Q.What is the default Simple Network Management Protocol (SNMP) timeout used by Software Management? Can I configure it?
- Q.Can I configure TACACS or Radius authentication for devices that Software Management has upgraded?
- Q.Can I configure default privileges on terminal lines for Cisco IOS devices that Software Management has upgraded?
- Q.What is Job Approval?
- Q.What is the approver list?
- Q.Is the Job Approval policy enforced system-wide?
- Q.How do I configure Job Approval for Software Management?

- Q.Which Cisco IOS devices support bootldr images?
- Q.How do you identify bootldr image files?
- Q.How does the Software Management bootldr recommendation process work?
- Q.Where is the storage location of the bootldr image on the Cisco IOS device?
- Q.Does Software Management erase Bootflash if there is not enough free space on Bootflash?
- Q.Does Software Management change the configuration file for bootldr upgrades?
- Q.Can Software Management back up the current bootldr image while Software Management runs the Distribute Images job?
- Q.Does Software Management recommend bootldr images from Cisco.com in the Distribute Images function?
- Q.Can I upgrade modules on the device using advanced Distribution mode?
- Q.What image extension type are not supported in Software Management?
- Q.How can secured image upgrades be performed using Software Management?
- Q.How to use Reboot order configuration feature?
- Q.Is Image import from URL is treated as separate Job?
- Q.What is the best effort verification performed while distributing the image using Advance mode?
- Q.When does Software Management Application use SSH?
- Q.How can a protocol be Enabled/Disabled for a job?
- Q.How are devices upgraded using Secured Copy Protocol?
- Q.How much Disk space should be available while performing parallel image upgrade to large number of devices (more than 100)?
- Q.What is the swap file size required for Software Management application?
- Q.What Version of SCP is supported in Software Management application?
- Q.What are the pre requisites for using SCP for image upgrade?
- Q.Why is the job still running after I cancel it?
- Q.Why do I get an error message such as, `Navigation to other areas of this application is not available until the opened wizard is finished or canceled.`?
- Q.The Cisco.com profile window is sometimes filled with user and password and sometimes not. Why?
- Q.I am not able to select both sequential execution and sequential reboot at 'Schedule Job' step during distribution?
- Q.During Distribution by Advance flow, I get “Software Management application could not verify the flash inputs since there was no flash information available. Edit the expert input file and verify once again. If you do not edit the expert input file, you can continue with the task by clicking Next. However, the results may be inaccurate.”?
- Q.Why am I not able to see “Immediate” during software management jobs?
- A.Check if approval is enabled. If approval is enabled for Software Mgmt Jobs, you will not be able to schedule Immediate job.
- Q.I am not able to select the device (greyed box) at Software Management device selector page, but I'm able to select at inventory.

- Q.I am not able to select a user script which is in xxx path.
- Q.In ACS login mode. I'm not able to see links that I usually get to see.
- Q.In the Job Details Window (clicking on job ID in the Software Management Job Browser) I don't see the job status being updated.
- Q.What Validations are performed by Software Management before actual image distribution onto the device?
- Q.What is the minimum software version required to be running on the device for Software Management to upgrade the software?
- Q.Can I have a different script for each device in a job?
- Q.What device types can be used as remote stage device?
- Q.What device types cannot be upgraded using remote stage flow?
- Q.What are the pre-requisites for using the device as remote stage?
- Q.What Configuration changes are performed by Software Management on the remote stage device?
- Q.If I use the device as remote stage device does it impact the device's other functionalities? or what are the performance implications of using the device as remote stage device?
- Q.Are there any Bad version of IOS for Remote stage device?
- Q.Can I perform module upgrade (like Bootloader/mica/microcom etc.) using remote stage flow?
- Q.How many devices in a job can be upgraded using remote stage?
- Q.Can I perform Parallel upgrade using remote stage flow?
- Q.Can I perform Slam dunk upgrade using the remote stage?
- Q.What is the difference between Run-from-RAM and Run-from-Flash devices?
- Q.When does Software Management use the remote copy protocol (rcp) to transfer images?
- Q.How does Software Management ensure that file corruption does not occur during transfer?
- Q.After an upgrade, why does Software Management sometimes leave behind image files in the tftpboot directory?
- Q.How much temporary space do you need during image distribution?
- Q.Is Cisco.com connection mandatory for Software Management?
- A.Cisco.com connection is not mandatory for using basic Software Management functionality. Image distribution, library management, tracking software upgrade changes, and other functions can run without Cisco.com connectivity.
- Q.How does Software Management handle proxy environments?
- Q.Does Software Management support proxy with user authentication environments?
- Q.Why is the Cisco.com filter option on the Software Management Edit Preferences screen not provided for Catalyst or Cisco 700 Series images?
- Q.How come the Cisco.com filter option does not work in LS1010 devices?
- Q.Can I configure Software Management to retrieve images from a Cisco.com mirror site rather than the main Cisco.com site?
- Q.Why I cannot download crypto images?
- Q.How does Software Management verify the integrity of the images after importing them from Cisco.com?

- Q.Why does the Flash size displayed in the Add Image to Repository (Source:Cisco.com) function not match the actual size for some Cisco IOS devices?
- Q.What is a Dual Flash Bank device?
- Q.Does Software Management support software upgrades on dual RSP-based systems?
- Q.Why does Software Management require static IP routes or dynamic IP routing protocol for configuration for the upgrade of a run-from-Flash (RFF) partition on a Single Flash Bank (SFB) device?
- Q.Although the configuration of the Single Flash Bank (SFB) device includes an IP default gateway, why does Software Management not upgrade the device?
- Q.How do you change the IP default gateway configuration to allow Software Management to upgrade a device?
- Q.Why does Software Management require Cisco IOS Software Release 11.1 or later to run on a Single Flash Bank (SFB) device for an upgrade when you have configured the device with Frame Relay subinterfaces?
- Q.How is the job directory organized?
- Q.Which modem cards does Software Management support?
- Q.Which devices and software versions get support for the modem upgrades?
- Q.Which formats of Microcom firmware images does Software Management support?
- Q.Which format of Modem ISDN channel aggregation (MICA) portware do Cisco 3600 devices support?
- Q.Why does the Undo option not receive support for modem upgrades?
- Q.What connection mechanism does Software Management use for modem upgrades?
- Q.Does Software Management erase Flash for modem upgrades if there is not enough free space on Flash?
- Q.What is CIP?
- Q.Which devices support the Channel Interface Processor (CIP) microcode upgrade? What is the minimum software version necessary?
- Q.What is the minimum Channel Interface Processor (CIP) version that Software Management supports?
- Q.How can you import Channel Interface Processor (CIP) images to the Software Management library?
- Q.Is there support for the Undo option for Channel Interface Processor (CIP) upgrades?
- Q.What connection mechanism does Software Management use to upgrade Channel Interface Processor (CIP)?
- Q.Does Software Management change the configuration file for the Channel Interface Processor (CIP) upgrade?
- Q.Does Software Management supports CIP2?
- Q.In which order does Software Management upgrade modules on a Cisco Catalyst 5500/5000 device?
- Q.Does the Supervisor Engine card reboot after the upgrade of all modules?
- Q.Does Software Management determine if the newly deployed Supervisor Engine software or module software is compatible with the module types (or module hardware versions)?

- Q.Does Software Management support the upgrade of software on redundant Supervisor Engine card-based systems?
- Q.Does Software Management update the configuration file on Cisco Catalyst 5500/5000 devices during the software upgrade?
- Q.Does Software Management determine if the Supervisor Engine has the minimum required RAM to run a new image?
- Q.Are there restrictions on the downgrade of the software on the Supervisor Engine card and other modules?
- Q.Do you need to reconfigure the device when you downgrade the Supervisor Engine software?
- Q.In the 4.1(1) software release and later, Supervisor Engine III cards allow the storage of configuration files on Flash cards. Does Software Management preserve the backed up configuration files on Flash during a software upgrade?
- Q.Does Software Management allow you to upgrade epsboot images on Token Ring cards on Cisco Catalyst 5500/5000 devices?
- Q.Why does the Add Image to Repository (Source: Cisco.com) task not display Token Ring LAN Emulation (LANE) or Permanent Virtual Circuit (PVC)-only ATM software images?
- Q.How do you identify software image files for each of the ATM modules that Software Management does support? What are the file-name conventions on Cisco.com?
- Q.How can I make the Image Recommendation faster?
- Q.Why do the software version numbers that the `show module` command output displays from the Supervisor Engine command-line interface (CLI) and the version numbers that Software Management uses fail to match in some cases?
- Q.Does Software Management recommend the right ATM image for your ATM module type?
- Q.Should you use special images with Software Management for Cisco Catalyst 2900XL/3500XL devices?
- Q.How does Software Management handle image import functionality of TAR and bin types of images for Catalyst 2900XL/3500XL devices?
- Q.Why do software upgrades take longer on Cisco Catalyst 2900XL/3500XL devices?
- Q.How do you upgrade Route Switch Module (RSM) and LightStream 1010 (LS1010) module software on Cisco Catalyst 5500/5000 and 6500/6000 series switches?
- Q.Why does the Distribute Images task show all the images from Cisco.com for LightStream 1010 (LS1010) and Cisco Catalyst 8500 devices, even though you have configured Cisco.com filtering?
- Q.What is the minimum version that Cisco 700 series ISDN routers support?
- Q.What connection mechanism does Software Management use for Cisco 700 series upgrades?
- Q.Both Cisco 760 and 770 series devices run the same image. Why do you see only some images with versions later than 4.0(1) for 770 series devices but see all images for 760 series devices?
- Q.Why do you not see the option to reboot the device later on the Job Control page for Cisco 700 series routers?
- Q.Why do you not see the option to modify the boot commands on the Job Control page for Cisco 700 series routers?
- Q.Why does Software Management report download failures for some images even though the device runs the new image after the job completes?
- Q.In which order does Software Management upgrade modules on a Catalyst 5000 device?

- Q.Does Software Management check to see that the newly deployed Supervisor software or module software is compatible with the module types (or module hardware versions)?
- Q.Does Software Management support upgrading software on redundant Supervisor card-based systems?
- Q.What is the purpose of user scripts?
- Q.What if the user script crashes? Will it crash the Software Management job also?
- Q.When a Software Management job is scheduled, how is the baseline determined? When I distribute a job, is an automatic backup performed?
- Q.Can I set up a periodic download of Software Management images from Cisco.com?
- Q.Is browser timeout something I should consider when downloading?
- Q.What are crypto images?
- Q.How much temporary space is required during image distribution?
- Q.At what time will the images directory get created during the process of obtaining images from a device? Does this happen during the initial step?
- Q.How can I speed up Image Recommendation?
- Q.When a job is rejected, can it be edited or should I resubmit?
- Q.Can different group members edit jobs? What are the restrictions?
- Q.What is the role of the registry files?
- Q.How do I upgrade Network Analysis Module (NAM) using Software Management?
- Q.Can I change the job scheduled time?
- Q.How does Software Management handle the job status for an abnormally terminated job?
- Q.How does Software Management handle the job status of a pending job whose scheduled time has passed?
- Q.Why are some files left in the Software Management folder after Software Management has been uninstalled?
- Q.How can I enable or disable the SSH to Telnet fallback for Software Management jobs?
- Q.How can I export the images from SWIM repository to a local drive or a file system mounted to the LMS server?
- Q.Does Flash get erased if there is no sufficient space for Patch Distribution?
- Q.When I try to copy images, the Image Copy option fails indicating that the External TFTP server is inaccessible.
- Q.Can I specify the name of my input file as imagenames.txt when I try to export images using the Software Management (SWIM) CLI `exportimages` command?
- Q.I am getting timeout exception in cmdsvc (command service library) during a device connection/socket establishment. How do I change the default timeout and delays in cmdsvc?

Q. What are the high-level features of Software Management?

A. Software Management offers the following management functions:

- Software Distribution—Schedules download of software images to a single device or groups of devices. Hardware and firmware validation verifies whether the new image can run on the device. Image Upgrade can be performed in Sequential or in parallel. Also the In Parallel mode of upgrade device reboot can be controlled for the job.

  Provides several workflow to achieve this functionality

  - Distribute By Device [Basic]
  - Distribute [Advance]
  - Distribute by Image
  - Distribute by Remote Stage/ External TFTP server
  - Patch Distribution

- Software Repository—Builds and maintains a library archive of software images. Software images can be added to repository from,
  - Device—Allows to archive the current software images on the device
  - Cisco.com—Integrates with Cisco Connection Online (Cisco.com) to download software images.
  - File System—Allows to import an image from a directory accessible from the LMS server
  - Network—Allows the library to synchronize with the software images running on the devices. A periodic job can generate a list of images that are not in the library. You then have the option to import new images into the library and check them for discrepancies between software images running on the network and images in the library.
  - URL—Allows to download images from URL you specify.

- Upgrade Analysis—Determines the hardware upgrades required on network devices to enable them to run new software. Software Management allows analysis based on the location of image to be analyzed. Following locations are supported.
  - Cisco.com
  - Local Repository

- Job Management
  - Job Approval — Allows organizations to require approvals before allowing software upgrades.
  - Software Management jobs can be operated upon to,

    Retry

    Undo

    Cancel

    Stop

- Reports
  - Work order—Displays changes that will be made to network devices as part of the software upgrade.
  - Synchronization report—Displays which Software Management-supported devices are running software images that are not in the software image repository.
  - Audit trail—Tracks software changes made on the LMS server

Q. What privilege level is required to run Software Management functions?

A. Different options in Software Management require different levels of user privileges. Privilege levels are known as “roles” in LMS. For a list of LMS functions and required user roles, use the Permissions Report function (**Reports > System > Users > Permission**).

Q. How do I know which functions I can access in Software Management?

A. To find which functions you can access in Software Management:

- Select **Reports > System > Users > Who Is Logged On** to find your assigned roles.
- Select **Reports > System > Users > Permission** to verify which LMS and Software Management tasks you can run.

Q. Are there DNS dependencies for Remote Copy Protocol (RCP) to work properly for a device?

A. Yes. If there are multiple IP addresses configured on the device, all IP addresses on the device must be configured in the Domain Name System (DNS). Examples of devices with multiple IP addresses are those having many interfaces, with each interface configured with its own IP address, or a device that interfaces configured with primary and secondary IP addresses.

Configure the DNS so that all IP addresses are resolved to the same host name. The host name in the DNS should match the host name entered in the Device and Credential Repository.

Q. Can I use Remote Copy Protocol (RCP) to transfer images to devices?

A. Use the RCP transport protocol for image transfers only on Cisco IOS devices that support the CISCO-FLASH-MIB. Catalyst switches that run Supervisor software older than 5.2, and 700 Series devices do not support the RCP protocol.

The Cisco IOS devices can not use RCP if they only support OLD-CISCO-FLASH-MIB, (for example, MC3810) or if they do not support any Flash Management Information Base (MIB) (for example, RSP 7000 devices running Cisco IOS Software Releases 10.3-11.0).

Q. What connection mechanism does Software Management use to upgrade software?

A. Simple Network Management Protocol (SNMP) is the preferred mechanism used by Software Management to upgrade software. Some devices, however, cannot be upgraded using SNMP alone.

For such devices, Software Management uses a Telnet interface to do the upgrades. SNMP upgrades all Run-from-RAM Cisco IOS devices, Dual Flash Bank Run-from-Flash (DFB RFF) devices, and all Catalyst switches. If SSH is preferred for device connection then SSH is Used for connecting to the device.

Software Management uses Telnet to perform the following upgrades:

- Single Flash Bank Run-from-Flash Cisco IOS devices (SFB 2500s, 1600s, AS5200)
- RSP 7000 devices running Cisco IOS Software Releases 10.3 - 11.0
- Cisco 700 Series
- CIP, MICA, Microcom upgrades
- 3500/2900 series of devices
- 1900/2820 Series
- VPN 3000 Series of devices.

For complete list of supported protocols see Supported Device Table for Software Management.

Q. What is the default Simple Network Management Protocol (SNMP) timeout used by Software Management? Can I configure it?

A. Default retry is 2 and default SNMP time out value is 2. This value is configurable using **Admin > Collection Settings > Inventory > Inventory, Config Timeout and Retry Settings**.

Q. Can I configure TACACS or Radius authentication for devices that Software Management has upgraded?

A. Software Management supports upgrading devices that are configured for TACACS or Radius authentication. An exception is software upgrades on the Run-from-Flash partition if the device is configured with Radius protocol authentication. The Device and Credential Repository must be configured with the appropriate information to access the device.

Q. Can I configure default privileges on terminal lines for Cisco IOS devices that Software Management has upgraded?

A. Software Management upgrades software by using the Telnet interface or Command-Line Interface (CLI) on devices that do not support enough Management Information Base (MIB) instrumentation for software management.

Software Management uses Telnet to connect into the devices and executes privileged commands such as `copy tftp flash, copy flash tftp, erase flash, show version, copy flash modem` to perform upgrades.

Software Management modifies the configuration file using the Telnet interface to upgrade the software. For Software Management to work on a device, there are some restrictions on how default privileges and enable mode authentication are configured.

The restrictions apply to only those Cisco IOS devices that are managed by Software Management through the Telnet interface. Cisco 700 Series and Catalyst 5000/6000/4000 devices are not affected. Restrictions include the following:

- Software Management tries to run the above CLI commands from privilege level 15. The user must always configure an enable password/secret for privilege level 15, and the same password/secret must be entered in the Device and Credential Repository.

  If the device is configured with TACACS authentication for enable mode access, then the Enable TACACS user name and password must be entered in the Device and Credential Repository. The Enable User name and password authenticated by TACACS+ server always should receive a privilege level of 15.

- The default privilege level configured on a vty line must allow Software Management to run the CLI commands mentioned earlier as well change the configuration file on the device. The privilege level does not need to be 15, but setting the privilege level to 15 guarantees Software Management can always work on the device.

Q. What is Job Approval?

A. Job Approval allows an organization to require approvals before an administrator distributes software images. When an image distribution job is created, the administrator (or whoever creates the job) selects from a list of users who can approve the job.

For the job to run, one of the users on the approver list must approve it before its scheduled time. If the job is not approved, it will be rejected at the scheduled time.

Q. What is the approver list?

A. An approver list consists of user names in LMS who have the authority to approve software upgrades.

The following steps are required:

a. Create a approver (**Admin > System > User Management > Local User Setup > Add**).

b. Create the list by using the Create Approver List (**Admin > Network > Configuration Job Settings > Create/Edit Approver Lists**). Only users who have an Approver role can be added to the Approver List.

Q. Is the Job Approval policy enforced system-wide?

A. Yes. To create a job that does not require approval, disable the Software Management option.

Q. How do I configure Job Approval for Software Management?

A. To configure Job Approval, do the following:

a. Add the approver user.

b. Create an Approver List

c. Enable the Job Approval option

Q. Which Cisco IOS devices support bootldr images?

A. The following Cisco IOS device families support bootldr images:

- Cisco 4500 and 4700
- Cisco 7500, Route Switch Processor (RSP)-based 7000
- Cisco 7200
- Cisco AS5200, AS5300, and AS5800 Access Servers
- Route Switch Module (RSM) on Cisco Catalyst 5500/5000
- ESR 10K, 10K2 devices

See the Supported Device Table for Software Management application on Cisco.com for further information.

Q. How do you identify bootldr image files?

A. Bootldr image files follow this name convention, *platform-boot-mz.version*

An example is rsp-boot-mz.11.0(17)BT. If the second part (feature part) of the image file name contains “boot”, then the image is a bootldr image. The software library recognizes the file name and imports the image as a bootldr image. Bootldr images earlier than Cisco IOS Software Release 10.3 contain xboot in the feature part of the image. Software Management does not support such images.

Q. How does the Software Management bootldr recommendation process work?

A. Different hardware platforms in Cisco IOS Software have different bootldr images. For example, the bootldr image for the Cisco 4500 device is c4500-boot-mz; the bootldr image for the Cisco 7200 is c7200-boot-mz.

From the library, Software Management determines which bootldr images belong to the same family as the target device. Software Management then recommends the most current of all available images.

Unlike system software images, bootldr images do not have RAM requirements. Therefore, Software Management does not perform prerequisite matches between the device and the image.

Q. Where is the storage location of the bootldr image on the Cisco IOS device?

A. Software Management always uses the Bootflash card as the target Flash for the bootldr image. Software Management stores bootldr images on the Bootflash card only, even though Cisco IOS Software allows the store of bootldr images on a Flash card.

If you use other Flash cards for the store of bootldr images, problems can occur when you have stored other types of images, such as system software, Microcom, or Modem ISDN channel aggregation (MICA), in the same location.

Q. Does Software Management erase Bootflash if there is not enough free space on Bootflash?

A. If the Bootflash card does not have enough free space to store the new bootldr image, Software Management erases the Bootflash to make room for the new boot image. A verification warning alerts you of the Bootflash erase.

To see this warning, click the Failure/Warning link in the Status column of the Verify Image Upgrade window.

Software Management backs up and restores files on Bootflash with sizes of less than 1 MB.

Q. Does Software Management change the configuration file for bootldr upgrades?

A. Upon bootldr upgrade, Software Management changes the device configuration file such that the configuration file that downloads to the device contains:

Assume that the file name of the newly downloaded bootldr image is c4500-boot-mz.112-13.bin.

- no boot bootldr
- boot bootldr c4500-boot-mz.112-13.bin

Q. Can Software Management back up the current bootldr image while Software Management runs the Distribute Images job?

A. Software Management backs up the system software image only during the Cisco IOS Distribute Images job execution. The backup of bootldr images cannot take place. Use the add images function to import the bootldr image from device to library. (Select **Configuration > Tools > Software Image Management > Software Repository > Add**).

Q. Does Software Management recommend bootldr images from Cisco.com in the Distribute Images function?

A. Yes, Software Management does recommend the download of bootldr images directly from http://www.cisco.com during the Distribute Images job creation.

Q. Can I upgrade modules on the device using advanced Distribution mode?

A. No. Expert flow is not officially tested with all the possible module upgrade scenarios. Current implementation claims only system software upgrades using the expert flow.

Q. What image extension type are not supported in Software Management?

A. The following file/image types are not supported:

```
doc, txt, pdf, xls, ppt, jpg, jpeg, bmp, csv, mpg, au, xml, html, htm, java, class,
tex, ps, pps.
```

Q. How can secured image upgrades be performed using Software Management?

A. Current Version (4.1) supports new protocols such as, SCP and SSH. You can choose the appropriate protocols based on the device support.

For the devices that are upgraded using Telnet/SSH, new feature called Job based password can be enabled for scheduled job. You can specify a temporary password for the upgrade job and it will take precedence over all the credentials in the Device and Credential Repository.

Q. How to use Reboot order configuration feature?

A. This feature is applicable only in case of “parallel” mode of image upgrade. This feature can be used to perform sequential rebooting of devices. You can make this decision based on the network topology or any other deployment policy. The devices will be rebooted in the order specified by you.

Q. Is Image import from URL is treated as separate Job?

A. Yes, the workflow results in a job.

Q. What is the best effort verification performed while distributing the image using Advance mode?

A. Verification in Advance distribution mode is referred as the best effort verification because you can proceed to schedule the image upgrade even without the inventory data. This is designed to support devices that are not yet managed in CiscoWorks (pre-deployed devices).

Q. When does Software Management Application use SSH?

A. If the device type selected is to be upgraded using the CLI then Software Management application uses SSH (if opted in the preference). Even for fetching information required during the job creation stage, SSH is used.

Q. How can a protocol be Enabled/Disabled for a job?

A. Using the User Interface, **Admin > Network > Software Image Management > View/Edit Preferences**. Available protocols list the Software Management supported protocols. You have to add or remove the protocols to selected protocol order in order to enable or disable the protocol used for image transfer.

Q. How are devices upgraded using Secured Copy Protocol?

A. Image staging and other checks performed before the image distribution remains same for upgrade using SCP. The options such as Flash erasure, Delete, etc. are performed using Cisco Flash mib or old Cisco flash mib only.

The difference lies in the model used for image upgrade. LMS positions itself as a client for the Secured Copy options. Devices with SCP server are (like 2650XM) requested to initiate a file transfer job. The image is transferred from LMS to the devices.

Q. How much Disk space should be available while performing parallel image upgrade to large number of devices (more than 100)?

A. The amount of disk depends upon the number of images staged in the upgrade job. If the image selected is common for all the devices then disk space required is equal to size of the image. If different images are selected for each job then disk space required is the sum of all the images.

Q. What is the swap file size required for Software Management application?

A. LMS recommend a swap size of 2MB for managing 300 devices.

Q. What Version of SCP is supported in Software Management application?

A. Current implementation of SCP is based on the fcpsvc library that uses the SSHv1 stack. Current version of SCP supported is 1.0

Q. What are the pre requisites for using SCP for image upgrade?

A. The device should have SCP server Any image having 3DES feature has SCP server in it. SSH should be enabled on the device.

Q. Why is the job still running after I cancel it?

A. In Sequential mode, the job stops only after the image upgrade for the current device or module is finished. Canceling a running job does not cancel the software upgrade being performed at that time. The job stops only after the current upgrade is complete.

During this time, the Browse Job Status screen shows that the job is still running. In case of parallel upgrades, when a job is cancelled, the current set of devices being processed will be continued and not stopped. However, new devices will be processed only after the current devices have completed runing.

Q. Why do I get an error message such as, `Navigation to other areas of this application is not available until the opened wizard is finished or canceled`.?

A. Yes, you get this when you are in a wizard (you will see Back, Next, Finish, and Cancel when you are in a wizard at the bottom) and you click any of the other navigational links.

Q. The Cisco.com profile window is sometimes filled with user and password and sometimes not. Why?

A. If the Cisco.com user name and password is configured for you the same will be pre-populated. You can configure the Cisco.com credentials in the Cisco.com User Account Setup dialog box (**Admin > System > Cisco.com Settings > User Account Setup**).

Q. I am not able to select both sequential execution and sequential reboot at 'Schedule Job' step during distribution?

A. If you had selected execution to be sequential the same order applies to reboot. However, if the execution is parallel you will be allowed to select reboot sequential.

Q. During Distribution by Advance flow, I get “Software Management application could not verify the flash inputs since there was no flash information available. Edit the expert input file and verify once again. If you do not edit the expert input file, you can continue with the task by clicking **Next**. However, the results may be inaccurate.”?

A. You get this when there are no inventory information available for the device. You can expect this error for 2900, 3500, 3550 xl devices.

Q. Why am I not able to see “Immediate” during software management jobs?

A. Check if approval is enabled. If approval is enabled for Software Mgmt Jobs, you will not be able to schedule Immediate job.

Q. I am not able to select the device (greyed box) at Software Management device selector page, but I'm able to select at inventory.

A. Software Management support might not be there. See the Supported Device Table for LMS on Cisco.com

Q. I am not able to select a user script which is in xxx path.

A. The scripts are expected to be available in the specific path. The Software Management scripts are located at:
NMSROOT/files/scripts/swim (On Solaris and Soft Appliance)
NMSROOT\files\scripts\swim (On Windows)

Where *NMSROOT* is the CiscoWorks installed directory.

Q. In ACS login mode. I'm not able to see links that I usually get to see.

A. On the ACS server, check if some role to task mapping (tree) has got changed. The required Software Management task option should be selected on the ACS server for a particular role.

Q. In the Job Details Window (clicking on job ID in the Software Management Job Browser) I don't see the job status being updated.

A. The job status will not be updated, as only the job running status is getting refreshed.

Q. What Validations are performed by Software Management before actual image distribution onto the device?

A. Software performs the following checks before the job execution:

- Checks whether job file is Available at the job id and has required data in the format and prepares a list of devices to be upgraded in the job.
- Checks whether LMS License is valid
  - Whether license file is valid
  - Number of devices managed
- Removes all devices from the list which are not authorized for the user to perform image distribution.

  Removes all devices from the list which are in Suspended state or Conflicting state. Pre-deployed state devices are not removed.
- Checks for the proper pre/post job script (if any) ownership and permission
  - On Solaris and Soft Appliance, check is performed for `rwxr-x---` permissions for script file (0750)
  - On Windows, check is performed if the given script has write permissions for any non-admin and non-casuser
- Verifies that critical data required for image upgrade are present in the job file.

Q. What is the minimum software version required to be running on the device for Software Management to upgrade the software?

A. For Cisco IOS device minimum supported version is 11.0 where as for Catalyst Images Minimum supported version is 3.8.

For more details on minimum supported version for each device type refer to Supported Devices Table.

Q. Can I have a different script for each device in a job?

A. No, you cannot have separate script for each device.In Software Management 4.1, script is defined in admin preference option and is common for all Software Management jobs.

Q. What device types can be used as remote stage device?

A. All IOS devices with running image version >=12.0 version and complete CISCO-FLASH-MIB support can be used as Remote-Stage device.

Q. What device types cannot be upgraded using remote stage flow?

A. Content Engines (CE), Network Analysis Modules (NAM), Content Service Switches (CSS), and PIX.

Q. What are the pre-requisites for using the device as remote stage?

A. It must be an IOS device and it must be running >= 12.0 version and it must support CISCO-FLASH-MIB completely.

Q. What Configuration changes are performed by Software Management on the remote stage device?

A. tftp-server *flash-partiiton-name:image-nam*e alias *image-name* is the only command that will be added to the Remote stage device to make the image copied to Remote Stage device as accessible through TFTP from other devices.

Q. If I use the device as remote stage device does it impact the device's other functionalities? or what are the performance implications of using the device as remote stage device?

A. There will not be any impact on device's other functionalities and also they will no be any performance implications on the device that is used as Remote-Stage.

Q. Are there any Bad version of IOS for Remote stage device?

A. 12.3(5x) series.

Q. Can I perform module upgrade (like Bootloader/mica/microcom etc.) using remote stage flow?

A. No.

Q. How many devices in a job can be upgraded using remote stage?

A. There is no limit specific to remote stage flow.the number of devices in a remote stage job is same as that of other distribution flow.

Q. Can I perform Parallel upgrade using remote stage flow?

A. Yes

Q. Can I perform Slam dunk upgrade using the remote stage?

A. No. The image that you want to use must be in the Software Repository.

Q. What is the difference between Run-from-RAM and Run-from-Flash devices?

A. Most Cisco IOS devices load the software image from Flash to RAM when rebooting, then run the software from RAM. Such devices are called Run-from-RAM (RFR) devices. For these devices, the software image on Flash can be upgraded without rebooting the device.

Certain Cisco IOS devices (namely 2500s, 1600s, and AS5200s) run the system software image directly from Flash. These are Run-from-Flash (RFF) devices. The Flash partition in which the current image is stored is the RFF partition, which is read-only.

Software Management supports upgrading software images on RFF partitions by using a procedure called Rxboot upgrade. Before upgrading, reboot the device and put it into Rxboot mode, which makes the RFF partition available to write a new software image.

Q. When does Software Management use the remote copy protocol (rcp) to transfer images?

A. Generally the order defined in selected protocol list will be used for transferring (to upload and download) Cisco IOS® Soft wares. If RCP is in the top of the selected protocol list then RCP is used as the first protocol for image transferring on to the devices that support CISCO-FLASH-MIB.

Check the supported protocol list for the device to find out whether device supports RCP or not. Cisco Catalyst 5500/5000 switches and Cisco 700 series devices do not support rcp. Cisco IOS devices that do not support rcp include the Cisco 7000 series (route processor [RP]-based 7000 only) and MC3810.

All other Cisco IOS devices support the rcp protocol.

Q. How does Software Management ensure that file corruption does not occur during transfer?

A. Software Management computes the checksum of the image file. Then, Software Management compares this checksum to the checksum from the device after the copy of the image file to the device Flash.

Software Management also verifies the size of the file on the Flash. If either the size or checksum do not match, Software Management aborts the distribution and marks the job status as an error.

Q. After an upgrade, why does Software Management sometimes leave behind image files in the tftpboot directory?

A. Software Management removes the image files from the tftpboot directory after the upgrade unless the TFTP fallback job option is set. If the TFTP fallback option is set, Software Management uploads the image from the device and leaves the image in the tftpboot directory for fallback.

Software Management also modifies the boot system commands on the device to add a fallback command to boot from the original image on the LMS TFTP server if the upgraded image does not boot.

Q. How much temporary space do you need during image distribution?

A. The amount of free space necessary depends on the image file size and the number of devices for simultaneous upgrade. If the TFTP fallback option is set, you need additional free disk space to keep the current image in the tftpboot directory. Both the tftpboot and temp directories use disk space.

Q. Is Cisco.com connection mandatory for Software Management?

A. Cisco.com connection is not mandatory for using basic Software Management functionality. Image distribution, library management, tracking software upgrade changes, and other functions can run without Cisco.com connectivity.

Cisco.com connectivity provides the additional benefits of obtaining images and their attributes from Cisco.com and viewing the status of outstanding bugs against the software images running on the devices in the network.

The following features of Software Management require Cisco.com connectivity:

- Adding image to Repository from Cisco.com. Software Management can import images for all supported devices.
- Distributing images directly from Cisco.com to devices, also called Recommend Images from Cisco.com. Without a Cisco.com connection, the Recommend Images screen Image list box will not show any images from Cisco.com when it creates the Distribute Images job.
- Cisco.com upgrade analysis.
- Cisco IOS image deferral processing.

Q. How does Software Management handle proxy environments?

A. Software Management uses HTTP protocol to communicate to Cisco.com about downloading images and their attributes. If you use an HTTP proxy for Internet connectivity, configure Proxy URL information in **Admin > System > Cisco.com Settings > Proxy Server Setup**.

Q. Does Software Management support proxy with user authentication environments?

A. Yes, Software Management support proxy that requires user authentication.

Q. Why is the Cisco.com filter option on the Software Management Edit Preferences screen not provided for Catalyst or Cisco 700 Series images?

A. During the Distribute Images task, Software Management communicates with Cisco.com to obtain a list of applicable images and their attributes. Based on this information, Software Management recommends an image.

There are many Cisco IOS images available on Cisco.com, which can cause a substantial delay in retrieving image attributes from Cisco.com. Some of these images will not be relevant to the user. Software Management filters the amount of images being considered to make a more meaningful and manageable subset.

For Catalyst and 700 devices, fewer images are available on Cisco.com than for Cisco IOS; therefore, it is not necessary to filter the images.

Q. How come the Cisco.com filter option does not work in LS1010 devices?

A. Although LS1010 devices run Cisco IOS images, there are some differences in how the LS1010 images are released. LS1010 images do not follow the Cisco IOS-type image releases like general deployment (GD), limited deployment (LD), and early deployment (ED).

Therefore, Software Management cannot effectively filter LS1010 type images. Nor does Software Management filter Catalyst 8500 Series images.

Q. Can I configure Software Management to retrieve images from a Cisco.com mirror site rather than the main Cisco.com site?

A. No. Although the mirror Cisco.com sites contain the images, they do not store image attributes, such as minimum RAM and FLASH requirement. This information is available only from the main Cisco.com site at http://www.cisco.com.

Q. Why I cannot download crypto images?

A. Crypto images are available only to authorized Cisco.com users. All users can view the images during the Recommendation stage but only users with the right privileges can download the image. Make sure that the Cisco.com Login user configured in CiscoWorks has permission to download crypto images.

Q. How does Software Management verify the integrity of the images after importing them from Cisco.com?

A. Software Management checks the validity of the downloaded images by comparing the MD5 checksum of the image with the MD5 checksum value retrieved from the Cisco.com database.

Q. Why does the Flash size displayed in the Add Image to Repository (Source:Cisco.com) function not match the actual size for some Cisco IOS devices?

A. Software Management does not erase files whose sizes are less than 1 MB on Cisco IOS devices because those files may be config files that are backed up to Flash partitions or .html files or Java applets used for management.

Software Management subtracts sizes of all files whose sizes are less than 1 MB from the size of the Flash partition. The result of the subtraction is displayed as the size of the Flash partition in the Software Management user interface.

The Software Repository Management window (**Configuration > Tools > Software Image Management > Software Repository**) displays the size of the largest Flash partition on the device. The size is displayed as an integer-truncated value in megabytes.

The Distribute Images screen displays information for all Flash partitions on the device. The values are displayed with two-decimal-digit precision.

The example below illustrates Software Management's behavior on a Cisco IOS device, which has two files whose sizes are 10 KB and 50 KB respectively.

The Flash card's total size is 8 MB. Because it has two files whose sizes are less than 1 MB, the Add Image to Repository screen displays the size as 7 MB. The Distribute Images screen displays the size as 7.94 MB.

```
enm-2502> show flash
System flash directory:
File Length Name/status
1 8089628 c2500-js-l.112-14.bin
2 10470 test_file1
3 52995 test_file2
8153288 bytes used, 235320 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

Q. What is a Dual Flash Bank device?

A. The Flash card can be partitioned into two equal banks. Each bank is called a Flash partition. A Flash card that is not partitioned is Single Flash Bank (SFB) and the device is called an SFB device. A device that has its Flash card divided into two partitions is a Dual Flash Bank (DFB) device.

When Flash is partitioned into two separate banks, they are named flash1 and flash2. Software image files have to be completely stored in a single partition, so the maximum size of a software image is limited by the total size of any Flash partition.

On a Dual Flash Bank Run-from-Flash (DFB RFF) device, Software Management supports upgrading the flash partition that does not contain the running image. In other words, Software Management cannot upgrade the RFF partition on DFB devices.

This is because the other partition, which can be upgraded directly, is the recommended partition for storing the new software image.

The AS5200 device has two Flash cards, Bootflash and Flash. The Flash is an RFF system and Bootflash is an RFR system. The Bootflash is intended for storing bootldr images on the AS5200 and flash is for storing Cisco IOS System Software.

Q. Does Software Management support software upgrades on dual RSP-based systems?

A. Software Management updates the software on the master RSP processor by copying the software image file to the master RSP Flash card (bootflash: slot0: slot1:) and updating the config file on the master RSP. Software Management cannot do a complete job of upgrading the software on the slave RSP processor.

Software Management can only copy the software image file to the slave RSP processor, but it cannot update the config file on that processor. Users will have to run a separate Distribute Images job to copy the software image file to the slave RSP processor.

Since Software Management cannot update the config file on the slave RSP processor, users must select **Don't touch config file** and select the No Reboot option in the job created for upgrading software on the slave RSP processor.

Q. Why does Software Management require static IP routes or dynamic IP routing protocol for configuration for the upgrade of a run-from-Flash (RFF) partition on a Single Flash Bank (SFB) device?

A. Software Management upgrades SFB devices that are in Rxboot mode. Rxboot mode does not support IP routing, IP bridging, or Simple Network Management Protocol (SNMP). The Rxboot image can support only one IP interface. Before the reboot of the device while in the Rxboot mode, Software Management determines the:

- Interface that connects the device to LMS servers. Software Management shuts down all interfaces except the one that connects to the LMS server.
- Default gateway IP address for the forward of all IP traffic when the device is in the Rxboot mode.
- Software Management queries the ipRouteEntry MIB variables ipRouteDest and ipRouteIfIndex to determine the default gateway IP address and the interface that connects.

  If the device configuration does not include static IP routes or dynamic IP routing protocol, the ipRouteEntry table is not set on the device. Consequently, Software Management cannot determine the default gateway and the interface that connects to LMS.

Q. Although the configuration of the Single Flash Bank (SFB) device includes an IP default gateway, why does Software Management not upgrade the device?

A. Software Management requires an IP default gateway address and an interface that connects. If you configure only the IP default gateway with the configuration command (ip default-gateway ip-address), you do not generate the ipRouteEntry MIB table on the device.

You can parse the IP default gateway from the configuration file; however, there is no reliable way to get the connecting interface from the device without the ipRouteEntry MIB. Without the ipRouteEntry MIB, Software Management does not allow upgrades, even if you have manually configured the IP gateway on the device.

Q. How do you change the IP default gateway configuration to allow Software Management to upgrade a device?

A. Use the IP default gateway configuration command to convert to a static IP route. Replace ip default-gateway gateway_ip_address with ip route 0.0.0.0 0.0.0.0 gateway_ip_address, which removes the ip default-gateway command from the configuration file. Check the output of the show ip route command to verify the correct configuration of a static IP route on the device.

Q. Why does Software Management require Cisco IOS Software Release 11.1 or later to run on a Single Flash Bank (SFB) device for an upgrade when you have configured the device with Frame Relay subinterfaces?

A. Releases earlier than Cisco IOS Software Release 11.1 do not include Frame Relay subinterfaces in ifTable and ipRouteTable in RFC 1213. Software Management requires information from these tables to perform Rxboot mode upgrades.

Therefore, Software Management requires Cisco IOS Software Release 11.1 or later to run on an SFB device when the device has Frame Relay subinterfaces.

Q. How is the job directory organized?

A. When Software Management schedules a job, it creates a new directory:

- On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/swim
- On Windows, *NMSROOT*\files\rme\swim

Where *NMSROOT* is the CiscoWorks installed directory.

The directory name is the integer ID of the job. (Example: /var/adm/CSCOpx/files/rme/swim/23, where 23 is the Job ID.)

The Job directory contains the following files depending upon the type of Software Management task:

Distribution Job	Image Import Job Image	Synchronization Job
• swim_debug.log	• swim_debug.log	• swim_debug.log
• workorder.html	• workorder.html	• workorder.html
• distribution.xml	• import.xml	• synchreport.xml
• PostOperation.txt	• PostOperation.txt	• jobinfo.xml
• SwOperation.txt	• SwOperation.txt	• synchReport.txt
• SummaryTable.tab	• SummaryTable.tab	
• Hostname.upgStatus	• Hostname.upgStatus	
• HostName_Config_Snap		

Where,

- swim_debug.log contains the debug information during the job execution.
- workorder.html contains the changes that user has chosen to perform with the job
- *deviceName*.upgStatus- a serialized file created on job completion for Retry and Undo options.
- PostOperation.txt used for all jobs scheduled through UI.

- SwOperation.txt indicates Job has been triggered. Absence indicate job has crashed for what ever reasons
- SummarTable.tab for UI purposes always exists for executed job.
- _Config_snap contains the Changes that are performed by Software Management on the original configuration.
- HostName_telnet.log for some device types only.

Q. Which modem cards does Software Management support?

A. Software Management upgrades Modem ISDN channel aggregation (MICA) and Microcom 56K modems.

Q. Which devices and software versions get support for the modem upgrades?

A. Support is available for Modem ISDN channel aggregation (MICA) portware upgrades on:

- Cisco AS5200 that runs Cisco IOS Software Release 11.3(2)T or later and Bootldr version 11.2(11)P or later.
- Cisco AS5300 that runs Cisco IOS Software Release 11.2(9)XA, 11.3(2)T, or later.
- Cisco 3640 that runs Cisco IOS Software Release 11.2(12)P, 11.3(2)T, or later.

Support is available for Microcom firmware upgrades on:

- AS5200 that runs Cisco IOS Software Release 11.2(10a)P or later.
- AS5300 that runs Cisco IOS Software Release 11.1(14)AA, 11.2(7a)P, or later.

Note Cisco AS5800 devices also have modems. However, the modem microcode for these devices is bundled with the system software only and receives upgrades as part of the system software upgrade.

Q. Which formats of Microcom firmware images does Software Management support?

A. The Microcom firmware for 56K modems is available in two formats:

  – Controller firmware and the Digital Signal Processor (DSP) code as two files, for example, mcom-modem-fw-xx.bin and mcom-modem-dsp-xx.bin.

  – A combination of firmware and the DSP code in a single format, for example, mcom-modem-code-xx.bin.

The Cisco AS5300 supports only the image combination. If the Cisco AS5200 runs a Cisco IOS Software release later than Cisco IOS Software Release 11.2(10)P, the AS5200 supports only the combination file format.

Software Management supports only the combination format files (for example, mcom-modem-code-xx.bin). Software Management does not support separate firmware and DSP code files. You cannot import the files to the software library.

Q. Which format of Modem ISDN channel aggregation (MICA) portware do Cisco 3600 devices support?

A. The 3640 digital modem network modules can run two types of modem microcode.

- 3600-Specific Modem Microcode File—This file has a 3600-specific header and should have the characters c3600-mica in the file name. Software Management does not support such files.
- Cisco AS5300 Modem Microcode File—In Cisco IOS Software Release 11.2(12)P, 11.3(2)T, and later, the 3640 supports the AS5300 microcode files directly and the 3600-specific microcode files.

  The AS5300 microcode files have Executable and Linking Format headers that contain the version and other information about the image file. Even though the microcode file formats differ between the 3600 and the AS5300, the actual microcode that downloads to the MICA modems is the same.

Software Management supports only AS5300 format files. Therefore, the earliest Cisco IOS Software release that the 3640 supports is Cisco IOS Software Release 11.2(12)P.

Q. Why does the Undo option not receive support for modem upgrades?

A. To support the Undo option, Software Management must determine the version of software that runs and identify the image file on the device that corresponds. The image file must be present in the library or available on Cisco.com.

In the case of modem upgrades, Software Management cannot precisely determine the current software version on the modems in all cases. Moreover, different modems can run different software versions, which makes the undo process difficult to support.

Q. What connection mechanism does Software Management use for modem upgrades?

A. Software Management uses Simple Network Management Protocol (SNMP) to initiate the modem image file transfer to the device Flash. After Software Management copies the image to Flash, Software Management uses the Telnet interface to the device to run a command line interface (CLI) command that downloads the code to the modems. (The command is `copy flash modem`.)

Q. Does Software Management erase Flash for modem upgrades if there is not enough free space on Flash?

A. Yes, if the target Flash card does not have enough free space for the store of the new modem image, Software Management erases the target Flash. Software Management does not erase the Flash card if:

- The upgrade of the system software does not occur within the same job as the modem upgrade.
- The target Flash partition for the modem upgrade contains the current system software image.

Instead, Software Management prevents the modem upgrade on that Flash partition. On the Cisco AS5200, the Bootflash card stores modem images, which can contain the bootloader image that currently runs.

If there is not enough free space to contain the new modem image, Software Management erases the Bootflash card. Back up and restore bootloader images in the case that an erase of the Bootflash is necessary for the upgrade of the modem image. Software Management issues a verification warning if Software Management needs to erase the Bootflash.

Q. What is CIP?

A. CIP stands for Channel Interface Processor card. This interface card allows you to connect the Cisco 7000 router to IBM or IBM-compatible mainframes.

Q. Which devices support the Channel Interface Processor (CIP) microcode upgrade? What is the minimum software version necessary?

A. Software Management supports CIP upgrades on Cisco 7000 and 7500 routers that run Cisco IOS Software Release 11.1(1) or later.

Q. What is the minimum Channel Interface Processor (CIP) version that Software Management supports?

A. Software Management supports CIP version 22.0 at minimum.

Q. How can you import Channel Interface Processor (CIP) images to the Software Management library?

A. The Add Images function (**Configuration > Tools > Software Image Management > Software Repository > Add**) does not support the import of CIP microcode images from Cisco.com.

a. You first must download the images to the file system on the LMS server.

b. Then, choose Add option with source as File System to import them to the software repository.

   Software Management does not recommend the download of CIP microcode directly from Cisco.com for an upgrade.

c. Populate the software Repository with modem images before you run the Distribute Images function.

Q. Is there support for the Undo option for Channel Interface Processor (CIP) upgrades?

A. No, there is no support for the Undo option for CIP upgrades.

Q. What connection mechanism does Software Management use to upgrade Channel Interface Processor (CIP)?

A. Software Management uses the Telnet interface to the device to copy the CIP image to the Flash. Software Management uses TFTP (via Simple Network Management Protocol [SNMP]) for the configuration upgrade to add the boot command to load CIP microcode.

Q. Does Software Management change the configuration file for the Channel Interface Processor (CIP) upgrade?

A. To load the new CIP microcode, the CIP upgrade process adds these configuration commands:

```
microcode cip flash new_cip_image_name
microcode reload
```

Q. Does Software Management supports CIP2?

A. Yes, Software Management supports CIP2 images for CIP supported device types.

Q. In which order does Software Management upgrade modules on a Cisco Catalyst 5500/5000 device?

A. Software Management upgrades the Supervisor Engine module on the device before other modules. Software Management upgrades the remainder of the modules in slot-number order. For example, Software Management upgrades the module on Slot 3 before Slot 5.

Q. Does the Supervisor Engine card reboot after the upgrade of all modules?

A. If you elect to reboot devices immediately after the upgrade of software, Software Management reloads the Supervisor Engine card. The reload of the card results in the reload of all modules, before the upgrade of software on other intelligent modules. This process supports instances in which the new module requires a newer version of Supervisor Engine software.

If you choose not to reboot the device after the download of software, you then must reload the Supervisor Engine module manually. You also should consider that software that you have newly loaded on a module may require new Supervisor Engine software.

If a new Supervisor Engine software is necessary, you should reload the Supervisor Engine module before you load the new software to the other intelligent modules (such as ATM, FDDI, and Token Ring).

For example, you may download 3.1(1) FDDI software and 4.1(1) Supervisor Engine software in a single job. The 3.1(1) FDDI software may require 4.1(1) Supervisor Engine software. Then, you must reset the Supervisor Engine module before you can upgrade the FDDI software. In such cases, you must have already chosen the Reboot Immediately option.

Q. Does Software Management determine if the newly deployed Supervisor Engine software or module software is compatible with the module types (or module hardware versions)?

A. Software Management does not verify whether the newly deployed Supervisor Engine software supports all modules that are available on the chassis.

Usually, with the upgrade of Supervisor Engine software to a newer release, the software provides backward compatibility for all the modules that exist on the chassis. However, you should check the release notes of the Supervisor Engine software or module software to be sure that the software versions are compatible.

Q. Does Software Management support the upgrade of software on redundant Supervisor Engine card-based systems?

A. The redundant architecture of Cisco Catalyst devices ensures that when the device reboots after a software upgrade, the redundant Supervisor Engine automatically synchronizes all the data from the primary Supervisor Engine. No special processes are necessary.

Q. Does Software Management update the configuration file on Cisco Catalyst 5500/5000 devices during the software upgrade?

A. Software Management updates the configuration file on Catalyst 5500/5000 devices only when the device has a Supervisor Engine III card. Software Management updates the boot system commands and the config register value if necessary.

For Supervisor Engine I and II and other module upgrades, Software Management does not update the configuration file on the device. Instead, Software Management uses CISCO-STACK-MIB and TFTP to download the configuration file. Before Software Management changes the configuration file on the device, Software Management backs up the file to the Job Schedule directory.

The example below illustrates the Software Management update of the configuration file. Assume that a Supervisor Engine III card runs 3.1(1) software. Also, assume that the software image file is on slot0 with the name cat5000-sup3.3-1-1.bin.

The configuration file boot system commands before the upgrade are:

```
set boot system flash slot0:cat5000-sup3.3-1-1.bin
```

Software Management has upgraded the software to 4.1(2). The new software image is on the same Flash card as cat5000-sup3-4-1-2.bin. Software Management then performs these configuration updates:

```
clear all boot system all
```

This removes all boot system commands on the device.

```
set boot system flash slot0:cat5000-sup3.4-1-2.bin
```

```
set boot system flash slot0:cat5000-sup3.3-1-1.bin
```

The update modifies the BOOT environment variable on the Supervisor Engine III card. You can display the environment values on the device is you issue the show boot command from the Supervisor Engine command-line interface (CLI).

The config register update occurs only if the least significant four bits of the config register are not all set to "1".

For example, if the current config register value is 0x10F (with the least significant four bits all 1s), Software Management requires no change to the config register. If the current config register value is, for example, 0x111 or 0x11A, Software Management modifies the config register to 0x11F. The action generates this command:

```
set boot config-register 0x11F
```

Q. Does Software Management determine if the Supervisor Engine has the minimum required RAM to run a new image?

A. Software Management uses the Minimum Required RAM field for the Supervisor Engine software image. You can set this field when you import the image into the library. If you do not input a value in this field, Software Management uses this matrix to determine the RAM requirement:

Image Type Software Version RAM Requirement

- I, II sup < 2.1(1) 4 MB
- I, II sup > = 2.1(1) & < 3.1(1) 8 MB
- I, II sup8 > = 3.1(1) & < 4.1(1) 8 MB (8 MB RAM image)
- I, II sup > = 3.1(1) & < 4.1(1) 16 MB
- I, II sup > = 4.1(1) 16 MB
- III sup3 > = 3.1(1) 32 MB

Images that are 8 MB RAM are available in 3.1 and 3.2 software releases only for Supervisor Engine I and II cards.

Software Management tries to use CISCO-MEMORY-POOL MIB to determine the available memory on a device. The MIB is implemented from 4.1(1) Supervisor Engine software (on all different Supervisor Engine card types—I, II, and III).

- If a device runs the software that implements this MIB, Software Management performs a memory check between the image requirement and the size of DRAM that is on the device.
- If the device does not have enough RAM to run the image, Software Management generates a verification warning.
- If the current software on the device is earlier than 4.1, Software Management generates a generic verification warning about memory requirements.

Q. Are there restrictions on the downgrade of the software on the Supervisor Engine card and other modules?

A. You can downgrade Supervisor Engine card software to version 4.1(1) or later.

For example, if a Supervisor Engine card runs 4.2(1) software, you can downgrade the software to 4.1(2) or 4.1(1). However, you cannot downgrade the same Supervisor Engine card to 3.2(1b). If a Supervisor Engine card runs 3.2(2), you cannot downgrade the software to 3.1(1) or 2.4(1).

There are no restrictions for the downgrade of software on other modules, such as ATM, FDDI, and Token Ring. However, you should check the release notes of new software before you attempt downgrades on modules.

Q. Do you need to reconfigure the device when you downgrade the Supervisor Engine software?

A. When you downgrade Supervisor Engine software, parts of the configuration may be lost. You must check the configuration file and reconfigure as necessary. Use the backed up Software Management configuration file from the Job Schedule directory as a reference, or use the backed up configuration file from the Config Archive.

Q. In the 4.1(1) software release and later, Supervisor Engine III cards allow the storage of configuration files on Flash cards. Does Software Management preserve the backed up configuration files on Flash during a software upgrade?

A. Software Management erases a Flash card on Supervisor Engine III if the free space on the Flash card cannot store the target software image. Software Management does not erase files of sizes that are less than 1 MB during software upgrades. Since configuration files generally do not exceed 1 MB, Software Management does not erase these files.

Q. Does Software Management allow you to upgrade epsboot images on Token Ring cards on Cisco Catalyst 5500/5000 devices?

A. Software Management does not allow upgrades of epsboot images on Catalyst 5500/5000 devices. An epsboot string in the file names can identify epsboot images. Epsboot upgrades are not often necessary. You can perform the upgrades with the Supervisor Engine card command-line interface (CLI).

Q. Why does the Add Image to Repository (Source: Cisco.com) task not display Token Ring LAN Emulation (LANE) or Permanent Virtual Circuit (PVC)-only ATM software images?

A. The Add Image to Repository (Source: Cisco.com) function in Software Management displays software images for only a subset of these ATM modules:

- WS-X5153
- WS-X5154
- WS-X5155
- WS-X5156
- WS-X5157
- WS-X5158

Software images for these modules have version numbers that range from 2.2 to 3.2(8).

The WS-X5153 to WS-X5158 modules can run:

- ATM LANE
- PVC Traffic Shaping
- Token Ring LANE software images

Software Management also supports the upgrade of software on these modules:

- WS-X5161
- WS-X5162
- WS-X5165
- WS-X5167
- WS-X5168

However, no mechanism exists to import the images from Cisco.com directly into the Software Management software library for these modules. The software images that run on the modules support LANE on Ethernet, Token Ring, and PVC traffic shaping.

You must download the software images for these modules directly from Cisco.com. Then, import the images into the library with the Add Image to Repository function.

Software Management does not support software management on WS-X5166 modules.

Q. How do you identify software image files for each of the ATM modules that Software Management does support? What are the file-name conventions on Cisco.com?

A. ATM software image file names and version numbers determine on which modules the software image can run and identify the features that receive support. This table provides details on version numbers and file-name conventions.

Q. How can I make the Image Recommendation faster?

A. If you select Cisco.com image recommendation, try to limit the images by filtering.

Module IDs	Image Feature/Version	Image File Name Format (Example)	Version to Input in Software Management
WS-X5153 to WS-X5158	Ethernet LAN Emulation (LANE) 2.2 to 3.2(7)	cat5000-atm.ver_number 3.2(7) cat5000-atm.3-2-7.bin	2.2-3.2(7)
WS-X5153 to WS-X5158	Ethernet LANE 3.2(8)	c5atm-wblane.Cisco *_IOS_Software_rel_number* c5atm-wblane.113-2.5.WA4.4m.bin	3.2(8)
WS-X5153 to WS-X5158	Token Ring LANE 70.x	c5k-trlane.*ver_number* c5k-trlane.70-1-1.bin	70.x
WS-X5153 to WS-X5158	Permanent Virtual Circuit (PVC) Traffic Shaping 50.x	cat5000-atm-pvcshape.*ver_number* cat5000-atm-pvcshape.50-1-1.bin	50.x

Module IDs	Image Feature/Version	Image File Name Format (Example)	Version to Input in Software Management
WS-X5153 to WS-X5158	PVC Traffic Shaping 51.x	c5atm-wbpvc.*Cisco_IOS_Software_rel_number* c5atm-wbpvc.113-2.5.WA4.5.x.bin	51.x
WS-X5161, WS-X5162, WS-X5167, WS-X5168 (Truckee)	Ethernet LANE, Token Ring LANE, PVC Traffic Shaping 4.3, 4.4	c5atm-wtall.*Cisco_IOS_Software_rel_number* c5atm-wtall.113-2a.WA4.4b.bin	4(3), 4(4b)

ATM version-number conventions differ for different classes of ATM images. PVC, Token Ring LANE, and Truckee types of ATM images have unique version-number conventions. Software Management recognizes the version numbers that appear in the last column of the table. The input of an incompatible version number results in upgrade job failures.

ATM software release notes give the original version number of the image as well as a version number that is close to the Software Management version-number scheme. Check the release notes for version-number schemes.

Q. Why do the software version numbers that the **`show module`** command output displays from the Supervisor Engine command-line interface (CLI) and the version numbers that Software Management uses fail to match in some cases?

A. ATM module software for Cisco Catalyst devices uses Cisco IOS Software code as a basis. The software release for Truckee ATM modules as well as ATM software releases 3.2(7) and later use the Cisco IOS Software version-number scheme.

Software Management does not recognize the Cisco IOS Software version-number scheme for Catalyst ATM software images. Use the simple version-number scheme that appears in the table in this document. (See the Version to Input in Software Management column.)

Output of the **`show module`** command of the Supervisor Engine CLI and the **`show`** command on the ATM module can display different versions. If the software that runs on the Supervisor Engine is earlier than 4.1, the Supervisor Engine software does not recognize the Cisco IOS Software version-number scheme of ATM images.

Therefore, the Supervisor Engine displays a different version number than the output of the **`show version`** command on the ATM module.

Q. Does Software Management recommend the right ATM image for your ATM module type?

A. Yes, Software Management distinguishes different flavours of ATM images and recommends images based on current class of ATM card on the device.

Q. Should you use special images with Software Management for Cisco Catalyst 2900XL/3500XL devices?

A. The 2900XL/3500XL devices have three images:

- Regular Cisco IOS Software image.
- A TAR format HTML image that contains files for Visual Switch Manager.
- A TAR format image that contains both of these images.

Software Management uses the TAR format image that contains the Cisco IOS Software and HTML image. This image posts on Cisco.com, as do other images for 2900XL/3500XL.

When you use LMS for software upgrades, you should use images with the description Enterprise-IOS and HTML-Use. When you use Add Image to Repository from Cisco.com/Slam Dunk, you are able to see only these images.

Q. How does Software Management handle image import functionality of TAR and bin types of images for Catalyst 2900XL/3500XL devices?

A. For 2900/3500 device types Both .tar format and .bin format images are supported as system software. Network Synchronization option (Add image from network as source) will not be able import tar images because when the image downloads to the switch, the image distributes as small individual files on the Flash in different directories.

The switch command-line interface (CLI) does not provide commands to combine all the files and make a new TAR file that Software Management can then upload. Whereas the .bin image can be imported from the device as well as from the Network Synchronization option.

Q. Why do software upgrades take longer on Cisco Catalyst 2900XL/3500XL devices?

A. Software Management uses command-line interface (CLI) to download software to 2900XL/3500XL devices. Because the software on these devices has many HTML/gif files on the Flash, the software must first delete all the files and then proceed with the new software download. Deletion of the images takes time, which is why software downloads to devices can take up to 20 minutes.

Q. How do you upgrade Route Switch Module (RSM) and LightStream 1010 (LS1010) module software on Cisco Catalyst 5500/5000 and 6500/6000 series switches?

A. The RSM (also called the VLAN router) on a Catalyst 5500/5000 or 6500/6000 switch and the LS1010 module on a Catalyst 5500/5000 switch run Cisco IOS Software. RSMs and LS1010 modules have individual IP addresses and Simple Network Management Protocol (SNMP) agents. The LMS Inventory manages these modules as separate devices.

You can find the IP address of the RSM if you look at the Detailed Inventory report of the Catalyst 5500/5000 and 6500/6000 device that has the RSM on the chassis. The Module IP Address column in the Stack Modules section shows the IP addresses of all modules on the chassis.

If you do not find the addition of RSM or LS1010 to Inventory, you must first add the module as a device to Inventory before you attempt Software Management functions. Software Management functions that run on Cisco IOS devices also can run on an RSM or an LS1010.

Q. Why does the Distribute Images task show all the images from Cisco.com for LightStream 1010 (LS1010) and Cisco Catalyst 8500 devices, even though you have configured Cisco.com filtering?

A. Although LS1010 and the 8500 devices run Cisco IOS Software images, differences exist in the means of image release. The images do not follow the Cisco IOS Software image releases, such as general deployment (GD), limited deployment (LD), and early deployment (ED). Therefore, Software Management cannot effectively filter LS1010-type and 8500-type images.

Q. What is the minimum version that Cisco 700 series ISDN routers support?

A. For Cisco 760 Series ISDN routers, Software Management requires a minimum software version of 3.2(4) on the device. For Cisco 770 Series ISDN routers, the minimum version necessary is 4.0(1).

Q. What connection mechanism does Software Management use for Cisco 700 series upgrades?

A. Software Management uses the Telnet interface to the device to copy the 700 series image to the Flash. Software Management uses TFTP protocol. The LMS workstation is the TFTP client, and the device is the TFTP server.

Q. Both Cisco 760 and 770 series devices run the same image. Why do you see only some images with versions later than 4.0(1) for 770 series devices but see all images for 760 series devices?

A. When you load an image with a version earlier than 4.0(1) onto a 770 series device, the sysObjectID box changes to something other than Cisco-assigned. Also, LMS identifies the device as a non-Cisco device. Therefore, Software Management does not list images with versions earlier than 4.0(1) for Cisco 770 series upgrades.

Q. Why do you not see the option to reboot the device later on the Job Control page for Cisco 700 series routers?

A. There is no option to reboot the device later because 700 series routers reboot at the time of the new image download.

Q. Why do you not see the option to modify the boot commands on the Job Control page for Cisco 700 series routers?

A. Only one image at a time can appear on the 700 series devices, which means the boot command does not apply to these devices.

Q. Why does Software Management report download failures for some images even though the device runs the new image after the job completes?

A. Some new Cisco 700 series images use nonstandard name convention or nonstandard versions. Software Management incorrectly parses the version number from file names of those images. After the download of the new image, the device reboots.

Software Management retrieves the new image version from the device and compares that with the version that Software Management parsed. The two versions do not match. As a result, the software download appears to have failed, which generates as an error.

This problem occurs with c760-in.b-US.42-3.5.bin and c760-in.b-US.43.1.bin images for all countries.

You can resolve this issue by entering the correct version number when you import the image from the file system.

For example, for c760-in.b-US.42-3.5.bin, enter 4.2(3.5). For c760-in.b-US.43.1.bin, enter 4.3(1) as the version number.

Q. In which order does Software Management upgrade modules on a Catalyst 5000 device?

A. Software Management upgrades the Supervisor module on the device before other modules. The remainders of the modules are upgraded in the order of their slot number. For example, the module on Slot #3 is upgraded before Slot #5.

Q. Does Software Management check to see that the newly deployed Supervisor software or module software is compatible with the module types (or module hardware versions)?

A. Software Management does not verify whether the newly deployed Supervisor software supports all modules that are available on the chassis.

Usually, when Supervisor software is upgraded to a newer release, the software provides backward compatibility for all the modules that exist on the chassis. Users are encouraged to check the release notes of the Supervisor software or module software to make sure that the software versions are compatible.

Q. Does Software Management support upgrading software on redundant Supervisor card-based systems?

A. The redundant architecture of Catalyst devices ensures that when the device reboots after a software upgrade, the redundant Supervisor automatically synchronizes all the data from the primary Supervisor. No special processing is required.

Q. What is the purpose of user scripts?

A. User-supplied scripts are run before and after each device upgrade. They can be used for pre- and post validation checks. For example,

- The pre-upgrade script can check whether the device is accessible.
- The pre-upgrade script can check whether any users are connected to the access server. If the script finds that some users are connected, it can decide whether to disable the connections before proceeding with the upgrade.
- The post-upgrade script can check whether the device has upgraded successfully or not. Depending on the return value, Software Management either halts or continues with the rest of the upgrade job.

Q. What if the user script crashes? Will it crash the Software Management job also?

A. No, crashing of the script will not stop the Software Management job. Software Management executes the script in a different process space so the script crashing will not crash the Software Management job. However, Software Management will assume the script has failed.

Q. When a Software Management job is scheduled, how is the baseline determined? When I distribute a job, is an automatic backup performed?

A. There are two options that import images from the network to the Software Repository:

- Baseline tasks
- Synchronization

The baseline task (**Configuration > Tools > Software Image Management > Software Repository > Add > Network**) should be done only once as a part of the initial setup. This imports the images running on the network to your Repository.

To keep the Repository synchronized with any new images and changes caused by upgrades from sources other than Software Management, schedule a synchronization job to run periodically at appropriate intervals.

When this synchronization job runs, it looks for differences between the Repository and the network and allows any new images to be imported. During job distribution, Software Management backs up the current running image only if the option, Use current running image as tftp fallback image was selected when the job was created.

Q. Can I set up a periodic download of Software Management images from Cisco.com?

A. No. However, you can schedule a one-time import from Cisco.com to occur at a later time. Software Management does not allow you to automatically import images from Cisco.com to the Repository based upon your preferences.

Q. Is browser timeout something I should consider when downloading?

A. The Image Import option from Cisco.com and other devices can be done on a scheduled basis. Since this process runs as a background task on the server, the browser is not involved. However, when an Immediate Import job runs, it is performed as a foreground task, and the browser can still timeout.

Q. What are crypto images?

A. Crypto images are software images that use 56-bit Data Encryption Standard (DES) (or higher) encryption, and are subjected to export regulations. You must be a registered Cisco.com user, and be eligible and authorized to download such images.

Q. How much temporary space is required during image distribution?

A. The amount of free space that is required depends upon the image file size and the number of devices that are being upgraded simultaneously. If the `tftpfallback` option is set, additional free disk space is required to keep the current image in the tftpboot directory. Disk space is used both in the tftpboot and temp directories.

Q. At what time will the images directory get created during the process of obtaining images from a device? Does this happen during the initial step?

A. The software images directory gets created at the time of importing an image to the Repository; however, this should be transparent to you.

Q. How can I speed up Image Recommendation?

A. If you include Cisco.com for Image Recommendation, try to limit the images by filtering (**Admin > Network > Software Image Management > View/Edit Preferences**).

Q. When a job is rejected, can it be edited or should I resubmit?

A. No. You cannot edit or retry the rejected job. You should schedule a new job.

Q. Can different group members edit jobs? What are the restrictions?

A. The only job attribute that can be edited is the schedule time for non-Job Approval jobs. Any user who has the *Network Administrator* role defined can edit jobs or create new jobs; however, in the Job Approval model, the jobs can only be approved by users who are in the approver list specified during the creation of the job.

Q. What is the role of the registry files?

A. Software Management manipulates the Windows registry to automatically manage remote authentication during the **rcp** transfers on Windows. The following registry parameters are important for **rcp** service on Windows:

- *HKEY_LOCAL_MACHINE**SYSTEM*\CurrentControlSet\Services\crmrsh\Parameters\DEBUG

  Dictates the amount of debug information written in the Windows event log. (Default = 0, Maximum = 0xff)

- *HKEY_LOCAL_MACHINE**SYSTEM*\CurrentControlSet\Services\crmrsh\Parameters\rhosts

  Contains the list of authenticated hosts that can run remote commands on this machine. This list is automatically managed by Software Management.

- *HKEY_LOCAL_MACHINE**SYSTEM*\CurrentControlSet\Services\crmrsh\Parameters\rusers

  Contains the list of authenticated remote users that can run remote commands on this machine. This list is automatically managed by Software Management.

- H*HKEY_LOCAL_MACHINE**SYSTEM*CurrentControlSet\Services\crmrsh\Parameters\NoRuserCheck

  If set to 1, the remote user authentication is skipped or, in other words, any remote user from authenticated hosts can run commands on this machine. (Default = 0)

- *HKEY_LOCAL_MACHINE**SYSTEM*CurrentControlSet\Services\crmrsh\Parameters\NoRhostCheck

  If set to 1, the remote host authentication is skipped or, in other words, commands can be run on this machine from any remote machine.
  (Default = 0)

Q. How do I upgrade Network Analysis Module (NAM) using Software Management?

A. To upgrade NAM using Software Management:

- Ensure that the passwords for NAM's application and maintenance modes are the same.

  This is because Software Management takes the password information from Inventory. However, Inventory requires the application mode password to manage the device, and Software Management requires the maintenance mode password to upgrade the device. Therefore, the passwords for NAM's application and maintenance modes should be the same.

- For a NAM card present in a Catalyst 6000 device running CatOS, ensure that you set auto logout to a value that is high enough to allow the copying of the new image.

  This is because a NAM image is usually very large (nearly 65 MB), and it may take between 1 to 2 hours to copy this image during Software Management upgrade. We recommend that you set the auto logout to 0 to ensure that there is no auto logout while the image is being copied.

  To set the auto logout value, use the CLI command, `set logout 0`.

  For a NAM card present in a Catalyst 6000 device running IOS, ensure that you set exec timeout to a value that is high enough to allow the copying of the new image. We recommend that you set the exec timeout value to 0 (`exec-timeout 0 0`) on all the vty lines.

- Ensure that the htdocs directory under CSCOpx has enough space to stage the NAM image.

  During the NAM upgrade, Software Management first copies the NAM image from the *NMSROOT*/files/sw_images directory (On Solaris and Soft Appliance) or *NMSROOT*\files\sw_images (On Windows), to the *NMSROOT*/CSCOpx/htdocs/swimtemp (On Solaris and Soft Appliance) or *NMSROOT*\CSCOpx\htdocs\swimtempdirectory (On Windows), and then copies the NAM image to the NAM card, using HTTP.

- Ensure that NAM is added with the correct Local User (root) and its password.
- Ensure that NAM is added with the correct SNMP read/write community strings.
- Ensure that the switch, which contains NAM, is added with the correct attributes.

Q. Can I change the job scheduled time?

A. The job scheduled time can be modified only for pending jobs that do not require approval.

For a job that requires approval, you must cancel the job and retry or recreate the job.

Q. How does Software Management handle the job status for an abnormally terminated job?

A. Software Management checks the last modification time of the job results file for each running job when the Browse Job Status screen is displayed. If the results file has not been modified for the last six hours, Software Management assumes that the job was terminated abnormally (server reboot is a probable cause for the termination), and the job status is changed to Error.

Q. How does Software Management handle the job status of a pending job whose scheduled time has passed?

A. Software Management checks the scheduled time for each pending job when the Browse Job Status screen is displayed. If the current time is an hour past the scheduled time for starting the job, (lack of operating system resources is a probable cause for the job not running at the scheduled time), the job status is changed to Error.

Q. Why are some files left in the Software Management folder after Software Management has been uninstalled?

A. When uninstalled, Software Management does not remove the software images directory from the LMS server. The software images directory contains subdirectories for storing software images for various device families.

Q. How can I enable or disable the SSH to Telnet fallback for Software Management jobs?

A. To enable or disable SSH to Telnet fallback for Software Management jobs:

Step 1 Go to **Admin > Network > Software Image Management > View/Edit Preferences**.

Under the Distribution pane, there is a checkbox option, **Use SSH for software image upgrade and software image import through CLI (with fallback to TELNET)**.

Step 2 Do either of the following:

- Check this option, to enable the use of SSH for software image upgrade and software image import through CLI along with fallback to Telnet.
- Uncheck this option, to disable the use of SSH for software image upgrade and software image import through CLI along with fallback to Telnet.

Step 3 Click **Apply to save your changes.**

Q. How can I export the images from SWIM repository to a local drive or a file system mounted to the LMS server?

A. To export the image from Software Repository to a local drive or a file system:

Step 1 Select **Configuration > Tools > Software Image Management** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select images that you want to export, then click **Export**.

A confirmation message appears, `The selected images will be exported.`

Step 3 Click **OK**.

The Select directory to export window appears.

Step 4 Click on **Browse** to select a directory to which you want to export the selected images.

The Server Side File Browser dialog box appears.

Step 5 Choose the required directory and click **OK**.

The Image Directory field in the Select directory to export window displays the directory location which you had selected.

Step 6 Click **Next**

A progress bar appears indicating the progress of the export of images.

The Export Images Summary Report appears after completion of the export of the images with these details:

- Number of Selected Images
- Target Directory
- Summary

Step 7 Click **Finish**.

You have successfully exported the images to the selected directory.

Q. Does Flash get erased if there is no sufficient space for Patch Distribution?

A. No. Patch Distribution requires sufficient amount of free space in Flash and so it cannot be erased.

Q. When I try to copy images, the Image Copy option fails indicating that the External TFTP server is inaccessible.

A. If you come across this error, try any of these:

- Check whether TFTP service is running or stopped in the External TFTP server. If stopped, start it.
- Check if any security agent is preventing the application. If so register the application with security agent or disable the security agent.

Q. Can I specify the name of my input file as imagenames.txt when I try to export images using the Software Management (SWIM) CLI **`exportimages`** command?

A. Do not name your input files similar to arguments.

For example, if you specify

`cwcli swim exportimages -input` *`imagenames.txt`* **`-u`** *`admin`* **`-p`** *`admin`*

the following error message will be displayed

```
Invalid argument: imagenames
```

For example, you can specify the input filename as sample.txt

You can enter the following argument in your sample.txt

```
-imagenames image1,image2,image3,image4...........
```

So the **exportimages** command with input file will be:

```
cwcli swim exportimages -input sample.txt -u admin -p admin
```

Q. I am getting timeout exception in cmdsvc (command service library) during a device connection/socket establishment. How do I change the default timeout and delays in cmdsvc?

A. You can change the default timeout and delays in cmdsvc using the cmdsvc.properties file available in the following directory: *$NMSROOT/objects/cmf/data*

To change the default timeout and delay values:

Step 1 Go to the directory *$NMSROOT/objects/cmf/data*

Step 2 Open the **cmdsvc.properties** file.

Various timeout and delay values are listed in the file.

Step 3 Remove the Hash symbol (#) to uncomment a particular timeout or delay value.

Step 4 Remove the existing timeout or delay value.

Step 5 Enter new timeout or delay value.

Step 6 Save the **cmdsvc.properties** file.

Troubleshooting Software Management

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0013	Image Import option not supported for the selected devices	Image Import option is not supported because of device limitations. Check Software Management feature support matrix against the selected device platform.	None.
SWIM0014	No images to import into library from the selected devices	Either: • There are no images on the Flash Or • Cannot get Flash information from inventory.	Check the Inventory Detailed Device Report to ensure that Flash file information exists for the device. If report generation fails, schedule an inventory collection job and redo the Software Management image import job.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0019	Could not perform Image recommendation for the selected devices because of insufficient data.	Could not fetch Image information from the Inventory database.	Check the Inventory Detailed Device Report to ensure that Inventory data exists for the device. If report generation fails, schedule an inventory collection job and perform Software Management recommendation.
SWIM0020	Image Import option not supported for the selected devices	Image Import option is not supported because of device limitations. Check Software Management feature support matrix against the selected device platform.	None.
SWIM0021	Error encountered while parsing Job Data.	Either the Job Data file could not be located or the data for Image Upgrade was not provided.	Check whether you have access permissions to Job Directory, or re-create the job. If the problem persists, send all log files under job directory to TAC.
SWIM0027	Staging of the Image on the Remote Stage Device failed.	Image Copy to Remote Stage device failed because of SNMP Agent problems during transfer.	Check for any known bugs against the Image running on Remote Stage, or choose a different device. If the problem persists, send all log files under job directory to TAC
SWIM0028	Cleanup option on Remote Stage Device failed.	Image Erase or a Configuration download caused an error.	Check for any known bugs against the Image running on Remote Stage.
SWIM0034	Device reboot failed.	Either: • The device configuration for reboot is missing Or • The image downloaded onto the device is not suitable for the device to come up.	Check whether the `snmp-server shutdown` command is configured on the device. You can do any of the following: • Configure the devices and re-schedule the jobs. • Use NetConfig reload template to reload the devices. • Reload manually if you have only a few set of devices.
SWIM0036	Image addition to Software Library failed	Either an invalid image was imported into library or the image is corrupted.	Check whether the image is downloaded completely in the directory
SWIM0056	Invalid Remote Stage device selected.	Cannot use this device as Remote stage because of device limitations.	Check the Help documentation to see which devices can be used as Remote Stage.
SWIM0067	System software analysis failed	This is an unexpected runtime error.	contact Cisco TAC.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0089	Could not perform Image Import from Cisco.com on the selected devices.	Add Image from Cisco.com not supported for the device. This is because Cisco.com could not find the device platform in the supported list.	Check the Software Management feature support matrix against the selected devices platform.
SWIM0092	Could not perform Image Import from Cisco.com on the selected devices because of insufficient data.	The device information needed to fetch images from Cisco.com does not exist in Inventory.	Check the Inventory Detailed Device Report to ensure that Chassis information exists for the device. If Chassis information is missing, schedule an inventory collection job and retry the import workflow.
SWIM0093	Could not get Image information from Cisco.com	Could not connect to Cisco.com from CiscoWorks Server either because of incorrect Cisco.com credentials or missing proxy configuration.	Check whether Cisco.com credentials are correct. If they are correct, check whether the proxy server is configured with right proxy credentials. To configure proxy, go to: CiscoWorks Home page > Server > Security > Proxy Server Setup.
SWIM0101	The current version of the image on the device is different from the earlier version of the image.	This message is displayed when you retry a failed distribution job. This mainly happens when other jobs change the current running image of this device before scheduling the retry.	Try a new distribution job instead of retrying.
SWIM0118	Software Management application could not verify the inputs since there was no running image information. The device package may not have been installed. You can install it now and retry the task or you can install it before running the job. However, the results may not be accurate.	Advanced Distribution Flow: Either: • The selected device is not yet deployed in the network (pre-provisioned device) Or • It is still not supported by LMS.	Schedule the distribution job for a future date when the device is deployed Otherwise, the device package for this unsupported device will be installed and available in the LMS server.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0119	Software Management application could not verify the Flash inputs since there was no Flash information available. Edit the expert input file and verify it again. If you do not want to edit the expert input file, you can continue with the task by clicking **Next**. However, the results may not be accurate.	The selected device does not have any Flash related information. Generally the Flash details are present in the Inventory. You can check the Detailed Device Report to see the Flash details. If there are no Flash details for this device, Software Management will allow the user to schedule a distribution job without verifying the Flash details.	None.
SWIM0120	Software Management application did not verify the inputs since there was no running image information. If you find that the device package is not installed, install it before running the job. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate.	Advanced Distribution Flow: Either: • The selected device is not yet deployed in the network (pre-provisioned device) Or • It is still not supported by LMS.	Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the LMS server.
SWIM0121	Software Management application did not verify the Flash inputs as there was no Flash information. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate.	The selected device does not have any Flash related information. Generally the Flash details are present in the Inventory. You can check the Detailed Device Report to see the Flash details. If there are no Flash details for this device, Software Management allows a user to schedule a distribution job without verifying the Flash details.	None.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0122	Software Management application could not verify the inputs since there was no running image information available. Update your inventory and retry the task. If you do not want to update the inventory, you can continue with the task by clicking **Next**. However, the results may not be accurate.	Either: • The selected device is not yet deployed in the network (pre-provisioned device) Or • It is still not supported by LMS.	Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the LMS server.
SWIM0123	Software Management application could not verify the inputs since there was no running image information. Update your inventory and retry the task. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate.	Advanced Distribution Flow: The selected device is not yet deployed in the network (pre-provisioned device) or it is not supported by LMS.	Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the LMS server.

SWIM0125	An unexpected error has occurred. Contact Cisco support and attach the swim_debug.log file.	None.	Please contact Cisco TAC with the UI log available under:
			Windows:
			`CSCOpx\logs\swim_debug.log`
			Solaris and Soft Appliance:
			`/var/adm/CSCOpx/log/swim_debug.log`

SWIM0126	An unexpected error has occurred. Contact Cisco support and attach the swim_debug.log file.	None.	Please contact Cisco TAC with the UI log available under:
			Windows:
			`CSCOpx\logs\swim_debug.log`
			Solaris and Soft Appliance:
			`/var/adm/CSCOpx/log/swim_debug.log`

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0138	Cannot connect to the Job Manager. Check whether the jrm process is running properly. If it is not running, restart it and try scheduling the job again.	None	To check whether jrm is running, run command: `pdshow jrm` If jrm is down, restart CiscoWorks.
SWIM0139	Running image information is not available in Inventory for Remote-Stage device *Devicename*. Perform Update Inventory and check whether the required Flash data appears in the Detailed Device report. If it appears, retry the job; else, the data is not yet available from the device.	Either: • The Inventory is not updated Or • The image device running on the device is not populating the required Flash MIB information.	If data is not available from the device (due to bug in the image), upgrade the device with the higher version image. This higher image populates the Detailed Device report with the required Flash data.
SWIM0141	There is not enough free space on the repository to store the selected files. Please free up some disk space and retry the job.	Disk space is not sufficient on the server.	Free up some disk space and retry the job.
SWIM0142	RepositoryException while checking for disk space.	Disk space is not sufficient on the server.	Free up some disk space and retry the job.
SWIM0146	Could not get active image information. Either the device is not reachable or the sysconfigName OID information is not provided by the device.	A distribution job scheduled using Advanced flow for pre-provisioned devices has failed and you have tried a Retry task on this job. The pre-provisioned devices does not have running images and so this error message is displayed.	Ensure that the device is deployed or the device package for this device is installed before a distribution job is run on this device.
SWIM1001	The input parameters to the Image Distribution/Image Import/Image Activate are invalid.	You may have used incorrect Device Data for this task.	Check the application log file for more details.
SWIM1002	An error occurred in staging Image *Image Name.*	There may not be correct permissions for the image in the software repository or for the directories required for staging.	Retry the Image Upgrade option.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1003	SNMP Agent does not support the required instrumentation to get information about the Flash File system.	The SNMP Agent on the device does not support CISCO-FLASH-MIB/OLD-CISCO-FLASH-MIB.	Check for any known bugs related to these MIBs for the image version running on the device.
SWIM1004	Cannot get details about the Flash File system on the device.	There may be a faulty implementation of the MIB on the device.	Check the Bug Toolkit application for any known issues on the running image version.
SWIM1005	Flash Device or Partition does not exist on the device.	Either the Inventory data on the device is stale, or the selected Flash Device or Partition is invalid.	Trigger inventory collection on the device.
SWIM1006	Flash Partition does not exist on the device.	Either the Inventory data on the device is stale, or the selected Flash Partition is invalid.	Update the inventory collection on the device.
SWIM1007	You have specified the storage location on the device in an invalid format.	None.	Enter a valid format. For example: *moduleNumber\flashPartitionName:partitionNumber:filename* In case of Andiamo devices: *flashDeviceName://flashPartitionName/filename*
SWIM1008	You have specified an invalid format for the destination storage location.	None.	Enter a valid format. For example: *moduleNumber\]flashPartitionName:partitionNumber:filename* In case of Andiamo devices: *flashDeviceName://flashPartitionName/filename*
SWIM1009	Inventory reported enough space on Flash partition, but the distribution task found that the space is insufficient and requires erasure. The distribution task is being terminated.	The inventory data may be stale.	Update the inventory for the device and retry the job.
SWIM1010	The size of the partition selected to copy the image, is less than the image size.	None.	Select another partition to copy the image.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1011	Destination file size on storage location and the source file size are different.	This may be because of a network problem or a bug on the device.	Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.
SWIM1012	The file copied on the destination storage location is invalid.	The File Copy may have failed because of temporary network errors.	Retry the File Copy option.
SWIM1013	You have specified an invalid Job directory.	The destination directory that has been specified to copy the configuration file from the device is invalid.	Check whether the destination directory exists. If the directory exists, check whether there are write permissions. Also check whether there is enough disk space.
SWIM1014	Cannot generate configuration changes for Remote Stage option.	None.	Check for file permissions on the Job directory.
SWIM1015	Cannot generate configuration changes for activating the device.	None.	Check for file permissions on the Job directory.
SWIM1016	Cannot load new configuration to Remote Stage Device.	None.	Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.
SWIM1017	Cannot fetch configuration file from the device.	None.	Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.
SWIM1018	Cannot upload new configuration to the device during image activation.	None.	Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.
SWIM1019	Cannot reload the device. Device is not responding after the Reload command.	The image upgraded on the device has some issues.	Check the Bug Toolkit application for any known issues on the upgraded image version. Manually restore the device through the console.
SWIM1020	The device is not running the new image.	This may be because the new image is invalid or corrupted and the device has booted from another image.	Check the Bug Toolkit application for any known issues on the upgraded image version.
SWIM1021	Cannot get the IP Address of the server.	The DNS resolution of the LMS server may have failed.	Enable DNS resolution.
SWIM1023	Distribution task is not supported for this device.	The device packages that are installed may not be the correct package.	Check whether the correct device packages are installed on the server.
SWIM1024	Either the file already exists in the directory or the system cannot create this file.	Check whether another file with the same name already exists in the directory, or check whether there is enough disk space.	Create disk space and retry the task.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1025	The Configuration Register on the device does not allow you to boot the image from Flash.	The Configuration Register is not set to value 0x2102.	Change the Configuration Register on the device and retry the job.
SWIM1026	Cannot create a file and store the modified configuration.	There may not be sufficient permissions for the application to create the file, or there may not be enough disk space.	None.
SWIM1027	Error while fetching inventory information.	The data required for the selected task is either incomplete or missing in Inventory.	Check whether the Inventory data exists for the device in the Inventory Detailed Device Report. If there is no inventory data for the device, schedule an Inventory Collection job and retry the task.
SWIM1029	Cannot get the required inventory information for the device.	Either there was no inventory collection for the device or the device is not responding.	Update inventory for the device and retry the task.
SWIM1030	This is a Run From Flash (RFF) device, but the application cannot find the running image on the Flash.	Either the inventory has not been updated or the Flash file is deleted from the Flash.	Update the inventory and retry the task.
SWIM1031	No Candidate Images found for the running software.	Either: • Cisco.com is not included in the admin preferences Or • There are no applicable images in the software repository or Cisco.com	Check Admin preference or add images to software repository.
SWIM1032	Images obtained for Recommendation do not meet the hardware and software requirements of the selected device.	Either: • The Candidate Images were filtered based on the selected Admin Preferences Or • They did not meet the Flash/RAM/BootROM needed to run on the device.	Check the Admin Preference or add more images to software repository and retry thejob.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1033	Cannot find the Best-fit image for the device by applying compatibility checks.	Either: • The Candidate Images were filtered based on the selected Admin Preferences Or • They did not meet the Flash/RAM/BootROM needed to run on the device.	Check the Admin Preference or add more images to software repository and retry the job.
SWIM1034	No applicable images found for the device from the configured image sources.	Either: • Cisco.com is not included in the admin preferences Or • There are no applicable images in the software repository or Cisco.com	Check the Admin Preference or add more images to software repository and retry the job.
SWIM1035	Error while performing Recommendation option. Runtime error encountered while filtering images caused by a problem with a running image on the device.	None.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log
SWIM1036	Runtime error while performing Recommendation.	None.	Retry the job.If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log
SWIM1037	Error while fetching Flash Partition information.	Either: • The Flash information cannot be got from Inventory Or • There is a problem with the running image on the device.	Update the inventory and retry the task. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1038	No Read-Write Partition found on the device.	None.	Install a Flash device with a read-write partition and update the inventory.
SWIM1039	No Storage Recommendation is made for the device.	The selected device may not have sufficient free size partition to copy the image.	Check whether the selected device has the sufficient free size partition to copy the image.
SWIM1040	Cannot get the Flash information for the device.	Either: • The Flash information cannot be got from Inventory Or • There is a problem with the running image on the device.	Perform Inventory Collection and check whether the Flash information appears in the Detailed Device report. If so, retry the job. Else, data is not available from the device.
SWIM1041	This device upgrade requires opening an SSH/Telnet connection to the device.	Enable password is not configured correctly in Device and Credential Repository.	Make sure that the appropriate SSH/Telnet passwords are configured correctly in Device and Credential Repository.
SWIM1042	The amount of Bootflash on the device may not be enough to run the selected image.	The amount of Bootflash on the device may not be enough to run the selected image.	Specify the Bootflash size for the image by editing the attributes of the image stored in the software repository, increase the Bootflash size for the device, or select a different image for upgrading.
SWIM1043	Runtime error while performing Bootloader image verification.	Selected image version may not be in the standard version format.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log
SWIM1044	Bootflash partition will be erased before copying new image.	Selected Bootloader image does not fit in available space on Bootflash.	Select a different Bootloader image if available.
SWIM1046	Selected software does not fit in selected Flash partition.	Selected software image does not fit in the available space on Bootflash.	Select a different Flash partition for upgrading.
SWIM1047	Minimum software version required for MICA image upgrade is not known.	None.	Select the image in the software repository and update the minimum system software version using View/Edit Image Attributes option.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1048	The system software that is active on the device, cannot run the selected image.	The system software that is active on the device, is not compatible with the selected image.	Select a different image that can be upgraded with the current system software or upgrade the system software to *Software Version.*
SWIM1049	The selected image requires Flash to be erased during image upgrade.	None.	Check whether you have performed the necessary backup.
SWIM1050	Read-Write SNMP community string is not in the Device and Credential Repository.	The Read-Write SNMP community string is not available in the Device and Credential Repository.	Add Read-Write community string for the device in the credentials repository.
SWIM1051	Credential information cannot be obtained for the device.	Either: • The device is not managed in the LMS server Or • The device credentials are not correct or the device access privileges are insufficient.	None.
SWIM1052	Enable password is not configured for the device.	For Run For Flash (RFF) partition software upgrades, the Enable password must be configured.	Configure the Enable password in the credentials repository.
SWIM1053	Selected MICA Image is the same as the running image on the device.	The software version of the image is the latest on the device.	None.
SWIM1054	Error while checking the Telnet credential of the device.	None.	Make sure that the Telnet credentials for the device are correct.
SWIM1055	Selected Flash partition is ReadOnly.	Either the Flash partition is not write-enabled or the Read-Write partition does not exist.	Check whether the Read-Write partition exists. Set the Flash partition to be write-enabled.
SWIM1056	The method to update the software on the selected storage device is unknown.	None.	Select a different Flash partition, if available.
SWIM1057	The device will be put into Rxboot mode for the image upgrade.	None.	Select a different Flash device for the system software, if available.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1058	The selected software version has some known problems in the Flash MIB options which will make this application unable to perform software upgrades on the device.	None.	Upgrade the device manually or select a later software version, if available.
SWIM1059	Ensure Dial Shelf runs a compatible software image with the newly loaded Router Shelf software image.	The Router shelf software image is not compatible with the Dial Shelf software image.	See the Release Notes for the Router Shelf software image to make sure the current Dial Shelf software is compatible. If not, upgrade the Dial Shelf software.
SWIM1060	Cannot obtain the file size of the selected image.	The selected image may have been removed from Cisco.com.	Select another image for upgrading.
SWIM1061	Image available at Cisco.com is selected for upgrade. This image will be imported from Cisco.com when the job is run.	None.	Verify that connectivity to Cisco.com is available when the job is scheduled to run or select another image from the software repository.
SWIM1062	Selected image is already running on the device.	None.	Verify that this is the image you want to upgrade for the device. If so, no action is required. If this is not the image you want, select a different image.
SWIM1063	Minimum RAM requirement of the selected image cannot be determined.	RAM available on the device may not be enough to activate this image.	Update the minimum RAM value using View/Edit Image attributes or make sure that the device has enough RAM to activate the selected image or select a different image.
SWIM1064	RAM available on the device may not be large enough to activate the selected image.	RAM available on the device may not be large enough to activate the selected image.	Select another image or upgrade the RAM on the device and retry Upgrade.
SWIM1065	RAM available on the device may not be enough to activate the selected image.	RAM available on the device may not be large enough to activate the selected image.	Specify the RAM size for the image by editing the attributes of the image stored in the software repository, increase the RAM size for the device, or select a different image for upgrading.
SWIM1067	Runtime error while performing verification of the selected image.	None.	Select another image for upgrading. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1063	Minimum RAM requirement of the selected image cannot be determined.	RAM available on the device may not be enough to activate the selected image.	Update the minimum RAM value using View/Edit Image attributes or make sure that the device has enough RAM to activate the selected image or select a different image.
SWIM1068	Selected image does not have the minimum system software version required for the upgrade.	Selected image does not have the minimum system software version required for the upgrade.	Select another image with a version higher than 11.0.
SWIM1069	Feature subset of the running image cannot be determined. Select a different image.	This is a wrong message caused by a bug. The correct message is: `Feature subset of the selected image is a subset or equal to running software feature set.`	None.
SWIM1070	Feature subset of the running image cannot be determined. Select a different image.	This is a wrong message caused by a bug. The correct message is: `Feature subset of the selected image is a subset or equal to running software feature set.`	None.
SWIM1071	System software analysis failed.	Some unknown error has occurred during image analysis.	Please contact Cisco TAC with the UI log available under: Windows: CSCOpx\logs\swim_debug.log Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log
SWIM1072	Boot loader analysis failed.	Some unknown error has occured during analysis of the image.	Please contact Cisco TAC with the UI log available under: Windows: CSCOpx\logs\swim_debug.log Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log
SWIM1074	The selected image does not have any requirement to be analyzed. The image can be used to upgrade the device.	None.	None.
SWIM1075	Cannot find an image that is newer and can fit on the Bootflash.	None.	Add Bootloader images, to the Software Repository, with version greater than the running image version and that can fit into the Bootflash. Then retry the job.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1076	Cannot find a Read-Write Boot partition on the device.	Read-Write Boot partition is not available on the device.	Insert a read-write Bootflash on the device and update the inventory.
SWIM1077	Cannot find a Bootflash partition for the Bootloader image.	Bootflash partition is not available for the Bootloader image.	Insert a read-write Bootflash on the device and update the inventory.
SWIM1078	System and Bootloader images are getting upgraded to the same Flash partition.	System and Bootloader images are getting upgraded to the same Flash partition.	Select individual partitions for both, if available.
SWIM1079	Image version cannot be compared.	The image formats of both the images may not be compatible for comparison.	Check the format of the version. Select a different image for upgrading.
SWIM1080	Read-Write partition exists but you have selected the ReadOnly partition.	You may have selected Read only partition instead of Read - Write partition.	Select the Read-Write partition for upgrading.
SWIM1081	You have selected the Compressed System Image for Run From Flash (RFF) Upgrade.	Wrong image selected for Upgrade.	Select the correct image.
SWIM1082	Runtime error while comparing Modem Image.	Either a wrong modem image is selected for comparison or the modem image formats or not compatible.	Select a different Modem Image for upgrading. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log
SWIM1083	Cannot find an image that is newer and fits in the Flash.	None.	Add another image into software repository and retry the task.
SWIM1084	Cannot find a Minimum Flash Requirement for the device.	The Flash space available on the device may not be sufficient for the selected image.	Check whether the image fits on the device.
SWIM1085	The MinFlash Attribute is unknown for the selected image.	The selected image does not fit on the selected partition.	Check whether the image fits on the selected partition or select a different image.
SWIM1086	Device not supported.	The required device packages may not be installed on the server.	Check whether the appropriate device packages are installed correctly on the server.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1087	Cannot get the device representation.	The required device packages may not be installed on the server.	Check whether the appropriate device packages are installed correctly on the server.
SWIM1088	Runtime error occurred while creating the device upgrade data.	None.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log
SWIM1091	Minimum BootROM version of the selected image is not available in the software repository, or on Cisco.com.	The minimum BootROM value is not updated in View/Edit Image attributes for the selected image in software repository.	Update the minimum BootROM value using View/Edit Image attributes of the selected image in the software repository.
SWIM1092	Selected image does not have the minimum system software version required for system upgrade.	None.	Select an image that has a higher version than the minimum supported version. See the documentation for the Compatibility Matrix for Cisco IOS software.
SWIM1093	Cannot get Chassis Information from the inventory.	Check whether the Inventory data exists for the device in the Inventory Detailed Device Report.	If there is no inventory data for the device, schedule an Inventory Collection job and retry the task.
SWIM1094	SNMP-V3 parameters not in the Device and Credential Repository.	This could have been caused by any of the following: • The SNMP-V3 password is wrongly configured • The SNMP-V3 algorithm is wrongly configured • The SNMP-V3 engine ID is not configured in the Device and Credential Repository.	Check whether the SNMP-V3 password, SNMP-V3 algorithm, and SNMP-V3 engine ID is configured in the Device and Credential Repository.
SWIM1095	Error while checking the SNMP-V3 user name in the device context.	The SNMP-V3 credentials in the Device and Credential Repository is not up to date.	Update the SNMP-V3 credentials in the Device and Credential Repository and retry the task.
SWIM1096	Selected image is not applicable to this module.	The selected image is not applicable to this module.	Use the Cisco.com Upgrade Analysis feature to find an appropriate image.
SWIM1097	Selected Bootloader image is a lower version than the version of the Bootloader running on the device.	The Bootloader image version running on the device is the latest.	Check whether the higher version is available for upgrading.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1098	The selected image is lower than the running image on the device.	The image version running on the device is the latest.	Select a higher image for device software upgrade.
SWIM1099	Image Upgrade procedure may revert to the SSH/Telnet-based approach, based on the MIB instrumentation on the running image.	The SSH/Telnet passwords may not be configured in the Device and Credential Repository.	Make sure that appropriate SSH/Telnet passwords are configured in the Device and Credential Repository.
SWIM1100	Cannot find SNMP-V2 Read-Write Community String in the Device and Credential Repository.	The SNMP-V2 credentials may not be correctly configured in the Device and Credential Repository.	Check whether the SNMP-V2 credentials are configured correctly in the Device and Credential Repository.
SWIM1101	This Device Upgrade requires opening an SSH/Telnet connection to the device.	Enable password for the device is not configured in Device and Credential Repository.	Make sure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository.
SWIM1102	This Device Upgrade requires opening a SSH/Telnet connection to the device.	There was an error while checking the credentials of the device.	Make sure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository.
SWIM1103	Selected image may not be compatible to the device.	Image belongs to the same device family as the running image on the device. However, it is identified as non-compatible.	Check the Cisco.com documentation whether any caveats are identified for the selected image.
SWIM1104	The total space on the selected partition is not enough to upgrade all of the selected modules.	Multiple modules may be selected for upgrading on the same partition.	Select individual partitions for the selected modules, or deselect some modules.
SWIM1105	Image status for the selected image cannot be determined.	The selected image might be in the Deferred status.	Ensure that the image is not in the Deferred status. See the relevant documentation on Cisco.com before upgrading the images.
SWIM1106	Image selected for upgrade is compressed in .tar format. Flash will be overwritten while upgrading the image.	None.	Ensure that necessary backup jobs are completed before upgrading.
SWIM1107	This option requires *devicename* data in the inventory.	The required device information is not available in the inventory.	Perform Update Inventory and check whether the required data appears in the Detailed Device Report. If so, retry the job. Else the data is not retrieved from the device.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1109	Image status for the selected image is either Deferred or Not Supported.	Image status for the selected image is either Deferred or Not Supported.	Ensure that the image is supported by Software Management application. Check the documentation on Cisco.com before upgrading the image.
SWIM1110	.bin images are not supported for Stack Upgrade.	The .bin image has been selected for Stack Upgrade.	Select a tar image for Stack Upgrade.
SWIM1111	The available free space is not enough for upgrading this type of image.	Insufficient space for image upgrade.	Select a different image or free up some space. Update the inventory and retry the job.
SWIM1112	This module can be upgraded if managed independently.	This module can be upgraded only if it is managed as a separate device.	Assign an independent IP Address to this module. Manage it as a separate device and select that device to upgrade this module.
SWIM1113	Device Reboot failed or Reboot Verification failed.	The device is not running the new image after it is rebooted.	Verify the configuration used to load the new image. Verify whether the new image exists on the device in a valid Flash partition.
SWIM1114	The device cannot be reached after the reboot. Number of attempts to verify the device status has exceeded the maximum retry count.	Either: • An invalid image has been loaded onto the device Or • There are network connectivity problems.	Use the device console to determine if the device has reloaded with the desired image.
SWIM1115	Device is booted from TFTP server.	The backup running image is not supported.	None.
SWIM1116	Read-Write SNMP community string cannot be fetched from the Device Context.	The Read-Write community string is not available in the Device and Credential Repository for this device.	Add the Read-Write community string to the Device and Credential Repository.
SWIM1117	The selected image is incompatible and cannot run on the selected device.	The selected image is incompatible and cannot run on the selected device.	Use the Cisco.com Upgrade Analysis feature to find an appropriate image.
SWIM1118	Selected image has a lower version than the version of the running image.	The selected image has a lower version than the version of the running image.	Verify whether the correct image is running on the device. If so, no action is required. If not, select a different image.
SWIM1119	Telnet credentials are not present for this device. There was an error while checking the credentials of the device.	The SSH/Telnet passwords are not configured correctly in the Device and Credential Repository.	Ensure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1120	Cannot obtain the sysObjectID of the device.	Either: • The device did not respond when you added it to LMS Or • The device cannot be added correctly.	Manually enter the device type information in the Device and Credential Repository.
SWIM1122	Runtime error found during verification.	None.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log
SWIM1123	Telnet username not present for this device.	Either: • The Primary Credentials is not configured Or • It not configured properly for the selected device in the Device and Credential Repository.	Check whether the primary username is configured for the selected device, in Device and Credential Repository.
SWIM1124	Cannot copy the image from Flash with return code of *Code*.	None.	Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.
SWIM1125	Cannot copy the image from Flash with return code of *Code*.	None.	Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.
SWIM1126	Image copy to module failed with return code of *Code*.	None.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC) The debug logs are available at this location: On Windows: *NMSROOT*\files\rme\jobs\swim*JobID* On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/*JobID*
SWIM1127	Cannot connect to device through SSH/Telnet because of *Device*.	The SSH/Telnet credentials may not be correctly configured in the Device and Credential Repository.	Check whether the SSH/Telnet credentials are correctly configured in the Device and Credential Repository.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1128	Cannot disconnect from device because of *Device*.	the SSH/Telnet credentials may not be correctly configured in the Device and Credential Repository.	Check whether the device is configured correctly.
SWIM1139	Select any available Boot flash partition, for bootldr upgrade. We recommend that you use boot flash for bootldr upgrade.	This happens when the user has selected a Bootloader image for Distribution and a storage location other than Bootflash.	Select any available boot flash partition for bootldr upgrade.
SWIM1150	Could not get Command Service instance for device *DeviceName* because of CmdSvc Exception.	Either: • The device login credentials in DCR are wrong or empty. Or • The SSH option is selected in the Swim Admin pane and the target device does not support SSH.	Check whether the Login credentials in DCR and Login credentials specified during job scheduling are correct.
SWIM1151	Could not connect to the device *DeviceName* because of CmdSvcException.	Either: • The device login credentials in DCR are wrong or empty. Or • The SSH option is selected in the Swim Admin pane and the target device does not support SSH.	Check whether the Login credentials in DCR and Login credentials specified during job scheduling are correct.
SWIM1161	RXBOOT credentials are not configured for the device. If TACACS is used by the device, configure RXBOOT Mode credentials in the credentials repository. This will be used to contact the device in RXBOOT Mode (if configured) for Run From Flash (RFF) devices.	RXBOOT credentials are not configured for the device in Device Credentials Repository (DCR). This will be used for Run From Flash (RFF) devices when connecting in RX boot mode.	If TACACS is used by the device, configure RXBOOT Mode credentials in the Device credentials repository.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1162	Error when recommending image for the device.	Swim recommends the image based on device ROM, RAM and Flash which it collects from LMS Inventory module. If the device is having a faulty hardware (FLASH) then this will not be available in inventory.	Check the Inventory Detailed Device Report to ensure that Inventory data exists for the device (like Flash Partition size). If not, check the device for a faulty hardware or a bug in device software.
SWIM1163	Image Import from Device failed because of some unexpected error.	None.	Please contact Cisco TAC with the Job logs available under: Windows: *NMSROOT*\files\rme\jobs\swim*jobID* Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/*jobID*
SWIM1164	Image Distribute to Device failed because of some unexpected error.	None.	Please contact Cisco TAC with the Job logs available under: Windows: *NMSROOT*\files\rme\jobs\swim*jobID* Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/*jobID*
SWIM129	Selected image does not fit on the free Flash size on the device. Selected storage partition will be erased during the distribution.	Either: The boot loader image is selected for upgrade (and no system software image is selected along with it) or The storage location is not erased for the boot loader image to be copied.	Since the system software is not selected for upgrade, ensure that running system software is not in the selected storage partition. Back up the running system software and ensure that the device boots from the backed up image in case the job fails.
SWIM1501	Supervisor cannot be downgraded to an image version less than 4.1(1).	This happens when you try to distribute a CATOS image lesser than 4.1(1).	If you continue to downgrade, the device may lose its configuration. Use a higher version.
SWIM1506	Cannot move file from *Location 1* to *Location 2*.	There may not be sufficient permissions for the application to move or copy the file, or there may not be enough disk space.	None.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1507	Cannot back up the running image.	Either the file name or the storage partition name specified for backup is invalid.	You can stop the job, manually back up the running image, and retry the job.
SWIM1508	Cannot copy image *Imagename* to storage partition *Partitionname* .	Either the filename or the storage destination is invalid or the device does not provide the required MIB instrumentation for copying an image.	Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.
SWIM1510	Runtime error while performing Reload on a device.	None.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*\files\rme\jobs\swim*JobID* On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/*JobID*
SWIM1518	Runtime error during configuration upload.	None.	Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*\files\rme\jobs\swim*JobID* On Solaris and Soft Appliance: /var/adm/CSCOpx/files/rme/jobs/swim/*JobID*
SWIM1525	Unknown package type.	None.	Check whether the module is supported in the Software Management Function and Device Support Matrix on Cisco.com.
SWIM1529	There is no module information available in the inventory for *devicename*.	There is no module information available in the inventory for *devicename*.	Update the inventory and retry the task.
SWIM1530	Storage not applicable for the module *modulename*.	This module does not support storage.	None.
SWIM1532	No read-write partition exists on the device to accommodate the selected image.	None	Create some free space.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1542	Minimum supported version for Supervisor is 3.8.	None.	Select a higher version of the image to upgrade.
SWIM1543	Selected image has the same or a lower version than the version of the running image.	The selected image has the same or a lower version than the version of the running image.	Verify whether the correct image is running on the device. If so, no action is required. If not, select a different image.
SWIM1546	The NVRAM size on the device may not be large enough to run the image.	The NVRAM size on the device may not be large enough to run the image.	Select a different image or upgrade the NVRAM on the device and retry the Upgrade option.
SWIM1547	Available NVRAM size on the selected image cannot be determined.	RAM size on this module may not be large enough to store this image.	Make sure the module has enough NVRAM to run the selected image. Else, select a different image or upgrade the RAM on the module.
SWIM1548	There are no software requirements found for the selected image.	None.	Select a different image.
SWIM1549	Verify that the new software selected is compatible.	Software Management cannot determine the features in the ATM software.	Check the Release Notes for the new software to determine if all the features in the old software are available in the new software.
SWIM1554	The selected image cannot be used to upgrade the device.	The device does not have any module that can run the selected image.	Select a different image.
SWIM1556	Select the Storage partition.	None.	None.
SWIM1560	Slot number corresponding to the module cannot be got from inventory.	None.	Update Inventory and retry the task.
SWIM2001	Telnet error while connecting to the device. Cannot connect to device %s.	Invalid access information in the inventory.	Verify the username and the passwords in Device and Credential Repository and retry the task.
SWIM2002	Cannot get details about Flash File system on the device.	Either the Flash device is not available or the Flash information format has changed.	None.
SWIM2503	Different images have been selected for upgrade of the Active and Stand-by processors. This may make the device unavailable.	None.	Select the same image for upgrade of Active and Stand-by CPUs.
SWIM3501	Cannot fetch device credentials for the selected device.	The credentials may not be configured correctly in Device and Credential Repository.	Check whether there are credentials are configured correctly in Device and Credential Repository.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM3502	Cannot fetch the credentials of the parent device, for the selected device.	The NAM device Supervisor is not recognized by the LMS Inventory.	Add the Supervisor of the NAM device to the LMS Inventory.
SWIM3503	Telnet credentials are not present for the parent device.	The Telnet credentials are not properly configured for the parent device.	Check whether the Telnet credentials are configured for the parent device.
SWIM3504	If Auto Logout is enabled on the parent device, it may get disconnected during upgrade. Configure No Auto Logout for the parent device.	None.	None.
SWIM3505	NAM images are large.	The disk space available is insufficient.	Ensure that there is enough disk space available in the htdocs/swimtemp directory under the CiscoWorks install directory.
SWIM3703	Selected image does not have the minimum system software version required for system upgrade.	None.	Select a different Image with a version higher than 11.3(0).
SWIM3705	This NRP2 is in ROMMON state. Cannot perform software upgrade on this device.	The NRP2 device is not in normal mode.	Manually bring the device into the normal mode and retry the task.
SWIM5001	Cannot connect to the device *devicename* using protocol.	The device may not be reachable or there is invalid access information in the Device and Credential Repository.	Verify whether the device is reachable and the credentials in Device and Credential Repository are correct and retry the job.
SWIM2002	Cannot get details about Flash File system on the device.	Either the Flash device is not available or the Flash information format has changed.	Done.
SWIM4602	Only image versions 6.2 or above are supported through AUS.	The image version in the device is less than 6.2.	Manually upgrade the device to a version higher than 6.2.
SWIM4800	The version running on the device is less than the minimum supported version.	None.	Manually upgrade the device to the minimum supported version or higher.
SWIM5003	Cannot copy the image.	Either the server address is incorrect or the image is inaccessible to the device.	Check whether the server address is correct and whether the image is accessible to the device.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM5004	Cannot initiate SNMPset option.	The SNMP Write Community String might be wrong.	Check whether the correct SNMP Write Community String is entered in Device and Credential Repository.
SWIM5005	Device reboot option failed.	The device is not configured for reboot. The command, `snmp-server system-shutdown`, should be in the running configuration on the device.	Modify the device configuration and retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*\log\swim_debug.log On Solaris and Soft Appliance: /var/adm/CSCOpx/log/swim_debug.log
SWIM5006	Device reboot option failed.	The device is not configured for reboot. The SNMP Write Community string might be wrong.	The command SNMP server system shutdown should be in the running configuration on the device. Modify the device configuration and check whether the Write Community string is configured on the device is same as the one that is entered in Device and Credential Repository.
SWIM5007	CPU switchover failed.	Either the SNMP set failed or the device is not in hot standby mode or the two CPUs are not running similar images.	Do any of the following: • Check the SNMP credentials in the Device and Credential Repository • Ensure that the device is in hot standby mode, • Ensure that the two CPUs are running similar images, before attempting the switchover.
SWIM5008	Device not responding after running the `switch cpu` command.	—	Check the Bug Toolkit application for any known issues on the running image version.
SWIM5009	Device is not in HotStandby Mode. Switch Operation terminated.	The Standby CPU may be down.	Bring up the standby CPU and retry the job.

Job Approval

This section provides the troubleshooting information for the Job Approval application:

Message ID	Error Message	Probable Cause	Possible Action
JBAP0001	Cannot enable approval for applications that do not have an Approver-List assigned to them	You have attempted to enable Approval without assigning a list to the application.	Go to the **Approval** > **AssignLists** screen and assign a list to the application. Enable Approval again.
JBAP0002	Specify a valid E-mail address.	You have entered an invalid E-mail-address.	Enter a valid E-mail address
JBAP0003	Select at least one job.	You have attempted to perform an action on a job without selecting a job	Select a job before performing an action on it.
JBAP0004	Select only one job.	You have attempted to view JobDetails, with more than one job selected	Select only one job.
JBAP0005	List {0} has no users. To save the list successfully, add users and click **Save**	This is not an error. This is an Information message when you adda list for the first time.	Add users before saving the list
JBAP0006	{0} is not a valid Approver. Enter a user with Approver role	You have attempted to add a user who has not been added as Approver in CMF.	You must first add the user as Approver into CMF. Only then can you add this user into LMS.
JBAP0007	Select an Approver, to change E-mail.	You are trying to save without selecting a user.	Go back and select a user.
JBAP0008	List {0} already exists.	You have attempted to add a list that already exists.	Add the list with a different list name.
JBAP0009	Could not approve/reject the job {0}. Verify that the database and mail server are running.	Either approve/reject mails cannot be sent, or the database is not running.	Make sure mail server is configured properly and that the database is running.
JBAP0010	Cannot reject a job without comments.	You have attempted to reject a job without giving reasons for rejecting	Add comments if you want the job to be rejected.
JBAP0011	Select a future start date.	You have selected a past date while changing a job schedule	Select a future date.
JBAP0012	Job {0} is changed successfully.	Not an error message	None.

Message ID	Error Message	Probable Cause	Possible Action
JBAP0013	Are you sure you wish to delete? Approval will be disabled for applications to which {list-name} is assigned.	Alert message before deleting – not an error message.	None.
JBAP0014	Enter a valid Approver-List name.	You may have entered invalid characters such as spaces in the Approver name.	Add a valid user-name
JBAP0015	{list-name} already exists.	You have attempted to add a list name that already exist	Select a different name
JBAP0016	{user-name} already exists.	You have attempted to add a user name that already exists.	Add a new user name. This field is case-sensitive.
JBAP0017	Are you sure you wish to delete? This will disable approval for applications having {user-name} as the sole approver.	Warning message for deleting a user. If you have enabled Approval for an application whose sole approver is this user, it will be disabled.	None.
JBAP0018	You have attempted an action without selecting a user. Select a user before performing the action.	User not selected.	Select a user before performing the action.
JBAP0019	You have attempted an action without selecting a list. Select a list before performing the action	List not selected.	Select a list before performing the action
JBAP0021	Cannot save a list that has no approvers in it.	No approver available for the selected list.	Add approvers before trying to save the list.
JBAP0022	Cannot change schedule for {0}. A runtime error occurred when you tried to change the schedule of the job.	None.	This exception will appear in the MakerChecker.log in the following location: *NMSROOT*/log (On Solaris and Soft Appliance) *NMSROOT*\log (On Windows) where *NMSROOT* is the CiscoWorks install directory. Contact Cisco Technical Assistance Center (TAC) with this log file.
JBAP0024	Cannot send approval E-mails. Make sure that SMTP Server is configured correctly.	None.	Go to **Admin > System > System Preferences** and configure SMTP Server correctly.

cwcli config

This section provides the troubleshooting information for the `cwcli config` commands:

Message-ID	Error Message	Probable Cause	Possible Action
CCLI0001	Could not get any devices to work on.	This problem occured because of any of the following: • Specified devices is not managed by LMS. • You have not used the correct Device Display name • DCR server is down	Do any of the following, depending on what caused the problem: • Specify valid devices that are managed by LMS • Use a valid Device Display name. • Use the `pdshow` command to verify whether the DCR server is running.
CCLI0002	The job could not be created since no device is available.	This problem occured because of any of the following: • You have entered invalid arguments for the command. • You have entered devices that are not managed by LMS. • CTMJrmServer and jrm are down. • ConfigMgmtServer process is down.	Do any of the following, depending on what caused the problem: • Enter valid arguments. • Verify that the devices you have entered are managed by LMS. • Use the `pdshow` command to verify whether the CTMJrm server and jrm are running. • The ConfigMgmtServer process should be up for the configuration Download and Fetch options.
CCLI0003	Could not get results for devices within the specified time interval	Less timeout is configured	Either: • Increase the timeout value using the `-timeout` option. Or • Use Configuration Archive Job Browser to see the results.
CCLI0004	Could not retrieve the Device Identification number for the device.	This problem occured because of any of the following: • Specified devices are not managed by LMS. • You have not used the correct Device Display name • DCR server is down	Do any of the following, depending on what caused the problem: • Specify valid devices that are managed by LMS. • Use a valid Device Display name. • Use the `pdshow` command to verify whether the DCR server is running.
CCLI0005	There are no archived configurations for this device	Sync Archive has not happened for the specified device.	Archive the configuration using the Sync Archive feature. For details on using the Synch Archive feature, see the Online Help.

Message-ID	Error Message	Probable Cause	Possible Action
CCLI0006	Cannot create a temporary file to store the running configuration.	This problem occured because of any of the following: • There is not enough space to create a file in your file system. • You do not have permissions to create a file in the specified location.	Do any of the following, depending on what caused the problem: • Verify whether there is enough space to create a file in your file system. • Verify whether you have permissions to create a file in the specified location.
CCLI0007	Cannot retrieve the configuration file from the archive.	The specified version does not exist in the archive.	Verify whether the specified version exists in the archive. Use the `listversions` command to see the available versions.
CCLI0008	Could not create a temporary file in DCMA temporary directory.	This problem occured because of any of the following: • There is not enough space to create a file in your file system. • You do not have permissions to create a file in the specified location.	Do either of the following, depending on what caused the problem: • Verify whether there is enough space to create a file in your file system. • Verify whether you have permissions to create a file in the specified location.
CCLI0009	Cannot get running configuration.	The archive does not contain any versions for the device.	Verify whether the specified version exists in the archive. Use the `listversions` command to see the available versions.
CCLI0010	Device has only one version archived.	Synch Archive has not happened for the specified device	Archive the configuration using the Synch Archive feature. For details on using the Synch Archive feature, see the Online Help.
CCLI0011	The specified version of the configuration does not exist.	You have entered an invalid version of the configuration.	Use the `listversions` command to see the available versions and enter an existing version
CCLI0012	No baseline templates exist for this device.	None.	Use the `listversions` command to see the available baseline templates.
CCLI0013	Data file does not contain any device.	None	Add the devices in the data file and try again
CCLI0014	The job could not be created because of the errors reported.	This problem occured because of any of the following: • You have entered invalid arguments. • The data file is missing some parameters.	Do either of the following, depending on what caused the problem: • Verify whether you have entered valid arguments. • Update the data file if there are missing parameters.
CCLI0015	You should not use the **-f** option with more than one device.	Multiple devices are specified for the command to be executed along with **-f** option	Use the `-input` option to specify the file for every device

cwcli export

This section provides the FAQs for the `cwcli export` tool:

Q. What does **`cwcli export`** do?

A. **`cwcli export`** is a command line tool that also provides servlet access to export inventory, configuration and change audit data. You can use this tool to export inventory, configuration archive, and change audit data for devices in LMS, in the XML format.

You can use the **`cwcli export`** command to generate the Inventory and Configuration data in XML format. In addition to this, you can also export Change Audit data.

See these topics in the Configuration Management Help:

- *Running cwcli export changeaudit* for the usage and XML schema details.
- *Running cwcli export config* for the usage and XML schema details.
- *Running cwcli export inventory Command* for the usage and XML schema details.

Q. What is ComputerSystemPackage Class?

A. It is the class that contains the InstanceIDs of Cisco-Chassis and Cisco-NetworkElement, and relates the two.

Q. Where does **`cwcli export`** collect the configuration information from?

A. **`cwcli export`** collects the running configuration data from the latest configuration in the Config Archive.

Q. Is the containment hierarchy in inventory schema exactly the same as that in CIM?

A. No. Although the containment hierarchy in inventory schema is based on Common Information Model (CIM), it does not follow the exact containment hierarchy because of the limitations in the LMS database schema.

Q. What is an XSD file?

A. XSD file is an XML based alternative to Document Type Definition (DTD). It is based on XML schema language which describes the structure of an XML document. An XML schema defines the legal building blocks of an XML document, just like a DTD.

An XML Schema:

- Defines elements that can appear in a document.
- Defines attributes that can appear in a document.
- Defines which elements are child elements.
- Defines the order of child elements.
- Defines the number of child elements.
- Defines whether an element is empty or can include text.
- Defines data types for elements and attributes.
- Defines default and fixed values for elements and attributes.

Q. What is the AdditionalInformation tag in the inventory schema used for?

A. The AdditionalInformation tag is provided to define information that is specific to a device. The inventory schema may not contain information for all the elements in all the devices supported by **`cwcli export`**. The AdditionalInformation tag addresses scenarios where the inventory schema does not have tags to define information that you want to collect for some of the elements in a particular device.

Q. How do I know what fields come under AdditionalInformation?

A. For this information, see the topic, Additional Information Table, in the Configuration Management Online Help.

Q. Where can I find information specific to a particular node which I can see in detailed device information but not in **`cwcli export`**.?

A. For this information, see the topic, Additional Information Table, in the Configuration Management Online Help.

Q. How can I make use of the servlet interface?

A. You must write customized scripts which could connect to the servlet. The arguments and options have to be specified in XML format.

For more details, see the section, Using cwcli Commands in the Configuration Management Online Help.

Q. How can I get data for some particular entity from devices which are managed by different LMS servers?

A. You have to write a script to connect to different LMS servers and aggregate all data into a single file. After you get the aggregated data, you can parse it and get the data for any required entity.

Q. While using the -m option, can I use more than one E-mail id?

A. No. You can use only one E-mail address at a time, when you use the **`-m`** option of the **`cwexport`** command.

Q. Where can I get the descriptions of each node in the schema?

A. You can find the descriptions in the Configuration Management Online help. See the topic Overview: cwcli export and sub-topics.

Q. Why am I getting parse error when trying to parse some of the output files?

A. Some of the classes in IDU and Optical switches contains some special characters with ASCII code larger than 160. Most of the XML parsers does not support these characters and hence fails to parse these characters.

To overcome this, you have to manually search for those elements with special characters and append CDATA as given in the example below:
If there is an element,
checksum ¢ûo */checksum*
you must change it to
checksum `<![CDATA[¢ûo ]]>` */checksum*

VRF Lite

Q. What is VRF Lite ?

A. VRF Lite is an application that allows you to pre-provision, provision and monitor Virtual Routing and Forwarding-Lite (VRF-Lite) technology on an enterprise network.

Q. What is Network Virtualization?

A. Virtualization deals with extending a traditional IP routing to a technology that helps companies utilize network resources more effectively and efficiently. Using virtualization, a single physical network can be logically segmented into many logical networks. The virtualization technology supports multiple virtual routing instances of a routing table to exist within a single routing device and work simultaneously.

Q. What is VRF-Lite ?

A. Virtual Routing and Forwarding - Lite (VRF - Lite) is the one of the simplest form of implementing virtualization technology in an Enterprise network. A Virtual Routing and Forwarding is defined as VPN routing/forwarding instance. A VRF consists of an IP Routing table, a derived forwarding table, a set of interfaces that use the forwarding table and set of routing protocols that determine what goes into the forwarding table.

Q. What are the pre-requisites to manage a device using VRF Lite?

A. The pre-requisites to manage a device in VRF Lite are:

1. The device must be managed by LMS.
2. The device must either be L2/L3 or L3 device
3. The devices failing to satisfy pre-requisite # 1 or #2, are not displayed in VRF Lite.

   The device must have the necessary hardware support. For more information on hardware support, see
   http://www.cisco.com/en/US/products/sw/cscowork/ps563/products_device_support_tables_list.html.

   If the device hardware is not supported then the device will be classified as Other devices
4. If a device does not support MPLS VPN MIB, it is classified as a capable device.

5. VTP Server must be support MPLS VPN MIB. If the VTP Server does not support MPLS VPN MIB, LMS will not manage VTP Clients.

Q. The device must be managed by LMS to exercise all the functionality of VRF. The desired device is not listed in the device selector for the VRF configuration workflows. What is the reason for a device not listed in the device selector?

A. A device is not listed in the device selector due to the following reasons:

All VRF Lite Configuration workflows like Create, Edit, Extend, Delete VRF and Edge VLAN Configuration.

A device will not be listed in the Device Selector, if a device does not satisfy the pre-requisites as mentioned in the Pre-requisites.

If VRF Lite Configuration workflow is either Edit VRF, or Delete VRF or Edge VLAN Configuration then a device will not be listed in the Device Selector, if a device is not participating in the selected VRF.

In the Readiness Report, a device listed as a supported device may be because it is not managed by LMS. You can check if a device is managed by LMS using the Device Management State Summary. You can access the Summary by selecting Device Management option.

In Extend VRF workflow, the devices listed in the Device Selector are the devices that are not participating in the selected VRF.

In Edge VLAN Configuration workflow, the devices listed in the Device Selector are only L2/L3 devices that are not participating in the selected VRF.

Q. What are the different categories in which the devices are managed by VRF Lite? Or what criteria are used by VRF Lite to categorize the devices in the network?

A. VRF Lite identifies the devices based on the minimum hardware and software support required to configure VRF on the devices.

Based on the available hardware and software support in the devices, VRF Lite classifies the devices into following categories:

- VRF Supported Devices– Represents the devices with required hardware and software support available to configure VRF on the devices.
- VRF Capable Devices – Represents the devices with required hardware support available. But the device software must be upgraded to support MPLS VPN MIB. For information on the IOS version that supports MPLS VPN MIB, refer http://tools.cisco.com/ITDIT/MIBS/MainServlet.

  VRF Lite classifies all the devices from Cat 3k and Cat 4k family of devices as VRF Capable devices as these devices do not have the required MPLS VPN MIB support.
- Other – Represents the devices without required hardware support to configure VRF. SysOID of the device needs to be checked.

Q. While performing the VRF Lite Configuration, VRF Lite application prompts the following messages:

"The device(s) with display name(s) are already locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time Or Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

Or

Selected Device(s) are locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time Or Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

The above messages appear even if no VRF Lite configuration is performed parallelly. Why do I get these messages?

A. The VRF Lite application prompts with these messages when some other configurations are performed simultaneously.

You can check the status of the configuration workflow using Resource Browser. The JOB Id/Owner column will give the details of the workflows currently running in the application.

These messages also appear if any VRF Lite configuration workflow is abruptly ended or an error has occurred while unlocking the device. You can release the locked devices only after ensuring that no other configuration workflows are running simultaneously. You can release the locked device using the Resource Browser option.

Note If you unlock a device which is participating in a configuration workflow, the configurations details will be overwritten or corrupted. By default, a lock will be released after two hours.

Q. Sometimes, while performing VRF Lite configuration, I get the following message:

The device(s) with display name(s) are already locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time Or Ensure the devices are not used by configuration workflows and free the devices from **CS > Admin > Resource Browser**.

Or

Selected Device(s) are locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time OR Ensure the devices are not used by configuration workflows and free the devices from Resource Browser.

Can I get the details of the user who has locked the devices to perform VRF Lite configuration?

A. You cannot get the details of user who has locked the devices to perform VRF Lite configurations.

Q. In the Create, Edit, or Extend workflow, the application do not list the Routing Protocols used while configuring VRF. The Routing Protocol information displayed is NA. What do I need to do to get the routing protocol configurations details?

A. When the Routing Protocol information displayed is NA, it means that the configuration details are not fetched successfully in LMS. You can schedule the Sync Archive job from **Configuration > Configuration Archive > Synchronization**.

Q. What are the details of the VRF Lite log files? In which location are the VRF Lite log files located?

A. The following are the details of the VRF Lite log files:

1. Vnmserver.log – This log file logs the messages pertaining to the VNMServer process.
2. Vnmcollector.log – This log file logs the messages pertaining to the VRF collection.
3. Vnmclient.log – This log file logs the messages related to the User Interface.
4. Vnmutils.log – This log file logs the messages pertaining to the utility classes used by VRF client and server.

The above-mentioned VRF Lite log files are located in the following location:

In Solaris and Soft Appliance : /var/adm/CSCOpx/log/

In Windows: NMSROOT\logs

Q. When is the VRF Collection process triggered?

A. **Manually:**

You can manually schedule to run the VRF Collection process by :

Providing the setting details using **Admin > Collection Settings > VRF Lite**.

Automatically:

If you enable the **Run VRF Collector After Every Data Collection** in the VRF Collector Schedule page. The VRF Collection process will be automatically triggered after the completion of Data Collection.

You can reach the VRF Collector Schedule page using **Admin > Collection Settings > VRF Lite**.

Q. After the completion of the Data collection process, the VRF Lite Collector failed to run, What is the reason for failure?

A. Check if the **Run VRF Collector After Every Data Collection** option is enabled in the VRF Collector Schedule page. You can reach the VRF Collector Schedule page from **Admin > Collection Settings > VRF Lite** page.

Q. What is the reason for VLANs not getting populated in the VLAN to VRF Mapping page in the Create VRFand Extend VRFworkflows ?

A. The VLAN to VRF Mapping page lists the links connecting the source and the destination device. The VLANs are not listed in fields displaying the links in the VLAN to VRF Mapping page because VRF Lite tries to find a free VLAN in the devices connected using a link based on the following procedure

1. An SVI, VRF Lite searches for free VLANs in the range 1- 1005
2. An SI, VRF Lite searches for free VLANs in the range 1006-4005

Q. Why do I see the VRF description for all VRF(s) in home page as “Discovered by VRF Lite” ?

A. While creating or extending VRF, the description that you have provided is deployed to the selected devices on which VRF is configured. But, the description provided while configuring or extending, is not read by the VRF Lite application. Instead, the VRF Lite application provides the default description for all VRFs as “Discovered by VRF Lite”.

Q. Why some port-channels are are not discovered in LMS?

A. VRF Lite does not support port-channel and GRE Tunnel. Also, Currently VRF Lite supports only 802.1Q

Q. What is tested number of devices support in VRF Lite?

A. In an Enterprise network, VRF Lite is tested to support the configuration of 32 VRFs with VRF configuration supported in 550 devices in your network. However, at a given time, you can select up to 20 devices and configure VRF using the Create, Edit and Extend VRF workflow.

Q. What are the property files associated with VRF Lite?

A. The following property files are associated with VRF Lite:

1. The property file used to provide the settings for Purge and Home page auto Refresh is:
   NMSROOT/vnm/conf/VNMClient.properties (On Solaris and Soft Appliance)
   NMSROOT\vnm\conf\VNMClient.properties (On Windows)
2. The property file used to provide the SNMP and VNMServer settings is:
   NMSROOT/vnm/conf/VNMServer.properties (On Solaris and Soft Appliance)
   NMSROOT\vnm\conf\VNMServer.properties (On Windows)
3. The property file that stores the SNMP Timeout and Retries that you have configured is:
   NMSROOT/vnm/conf/VRFCollectorSnmp.conf (On Solaris and Soft Appliance)
   NMSROOT\vnm\conf\VRFCollectorSnmp.conf (On Windows)

Q. In the Interface to VRF Mapping page for the Create, Edit and Extend VRF workflow, why are values for the IP Address and SubnetMask fields empty?

A. If the physical interface that links two devices is not configured with an IP Address, then the IP Address and the SubnetMask fields are empty.

Q. What is protocol ordering for configuration workflows?

A. Configuration workflow uses the protocol ordering similar to ordering used by NetConfig.

Choose the NetConfig as Application Name from using **Admin > Collection Settings > Config > Config Transport Settings** page. You can view the protocol ordering in the Transport Settings page.

Q. What is protocol ordering for troubleshooting?

A. Troubleshooting VRF workflow uses the protocol ordering similar to ordering used by NetShow in LMS.

Choose the NetShow as Application Name from using **Admin > Collection Settings > Config > Config Transport Settings** page. You can view the protocol ordering in the Transport Settings page.

Q. If you configure commands to be deployed to two different devices, will the commands be deployed parallelly or serially?

A. The commands will be deployed to multiple devices parallelly, where as a series of commands with-in a single device, will be deployed in serial manner.

Q. Which VRF Lite configuration jobs that are failed can be retried?

A. You can retry all the VRF Lite Configuration jobs which are failed. VRF Lite Configuration jobs are the jobs pertaining to Create, Edit, Extend, Delete VRF and Edge VLAN Configuration workflow.

Q. In the Troubleshooting VRF page, after selecting the source device, no VRFs are listed in the VRF List to troubleshoot. Why?

A. Initially, check if a VRF is configured on the selected source device. The VRF list in the Troubleshooting page enlists the VRF(s) configured in the selected source device as well as in the Global Table, which refers to the global routing table.

Q. Which interfaces are displayed in the Troubleshooting VRF page

A. When a VRF is selected then all the interfaces that are configured with the selected VRF in the corresponding device is listed.

If you select VRF as “Global Table”, then the application displays all the interfaces that are not configured to any VRF

Q. In some scenarios, the VRF configuration commands are pushed to unselected devices. What is the reason?

A. In the following scenarios, the VRF configuration commands are pushed to unselected devices:

The VLANs are created in the VTPServer by default. In any VRF Lite Configuration workflow, if you create a VLAN in VTP Client devices, then VRF Lite application finds the corresponding VTP Server and create VLANs in that device.

In Delete VRF workflow, the virtualized interface in the connecting device will also be deleted, even if the device is not selected.

Q. Why the FHRP and DHCP configurations are not shown in VRF Lite?

A. VRF Lite does not fetch the details for the FHRP or DHCP configuration from the device. Also, VRF Lite won't put the list of vlan(s) allowed on a trunk

The Protocols and DHCP Server details for existing or newly created SVIs are not fetched from the selected devices.

INDEX

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W