Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

Prime LMS Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2011 are the "August 2011 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100 
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

An RSS feed is available if you would like to be notified when new comments are posted.

Table of Contents

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

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

What's In This SBA Guide

About SBA

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

For more information, see the *How to Get Started with Cisco SBA* document:

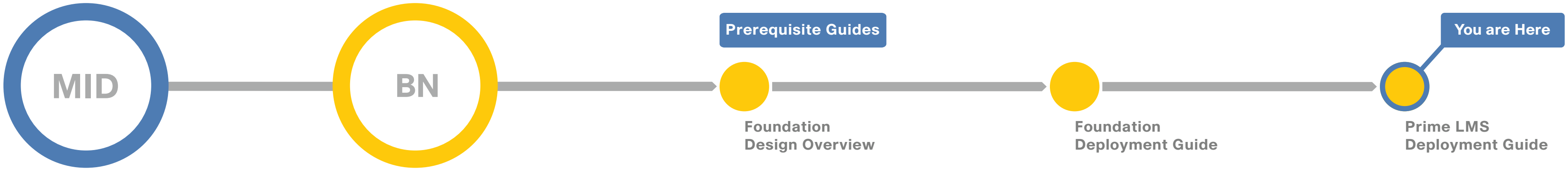
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

About This Guide

This *additional deployment guide* includes the following sections:

- Business Overview—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations' operations.
- Technology Overview—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- Deployment Details—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.


MID
BN
Prerequisite Guides
You are Here
Foundation Design Overview
Foundation Deployment Guide
Prime LMS Deployment Guide

Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

Introduction

Business Challenges

Data network management is a significant challenge to organizations that rely on their Cisco Borderless Network to enable efficiency and productivity for employees. The challenges of managing an enterprise network are beyond those of most other jobs, and the complexity compounds when there are multiple services running on the infrastructure. IT staff not only have to deal with demanding user issues but also have to efficiently address the needs of a growing network. These management needs fall into different use cases, such as network configuration, deployment, asset management, and troubleshooting. As the organization deploys new network hardware and architectural solutions, the management tools that the staff uses must explicitly support the hardware and solutions without requiring cumbersome workarounds or time-consuming patches.

An IT staff's top concern is to have a unified network management application that can help them address these needs, thus increasing the staff's productivity.

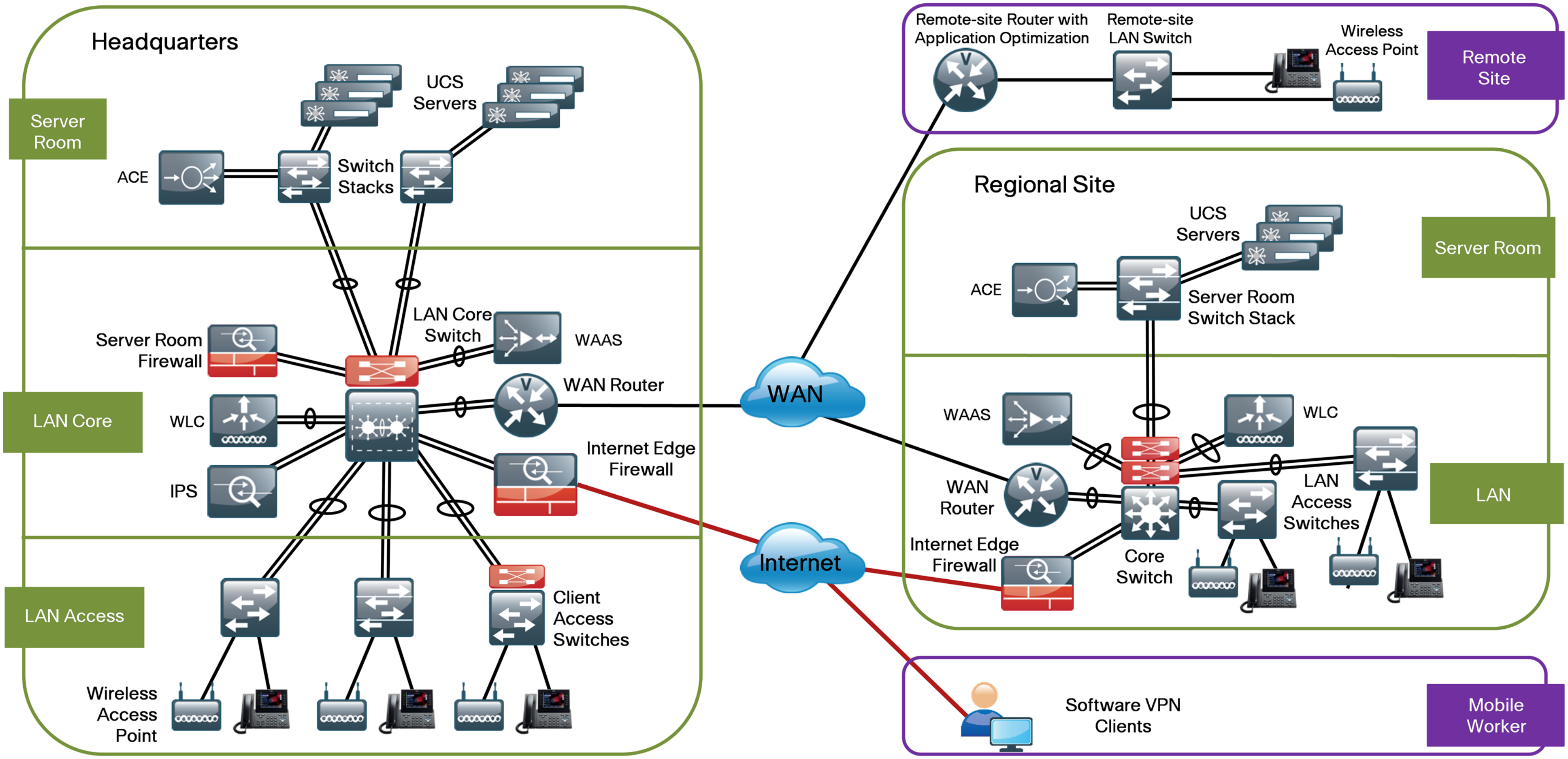
Technology Overview

Cisco® Prime LAN Management Solution (Cisco LMS) 4.1 allows an IT staff to address all these needs of a growing enterprise network. Cisco LMS provides an intuitive GUI that can be accessed from anywhere remotely and gives you a full view of a network use and performance.

Figure 1 depicts the Cisco Borderless Networks Smart Business Architecture (SBA) for Midsize Organizations. With such a network and services on top of it, network management applications like Cisco LMS play a critical role in day-to-day network operations. Cisco LMS is an integrated suite of management functions that simplify the configuration, administration, monitoring and troubleshooting of Cisco solutions. Built on top of the latest Web 2.0 standards, Cisco LMS allows network administrators to manage Cisco Borderless Networks for midsize organizations through a browser-based interface that can be accessed from anywhere at anytime within the network.

Notes

Figure 1 - Borderless Networks for Midsize Organizations overview



This guide adds to the example configuration already built in the core Cisco SBA document. This supplemental guide includes:

- Step-by-step procedures for installing and deploying Cisco LMS.
- Detailed descriptions of how you can monitor and troubleshoot your enterprise network.
- Templates that you can use to deploy global configurations across your networks.

The following sections describe the tasks this guide covers.

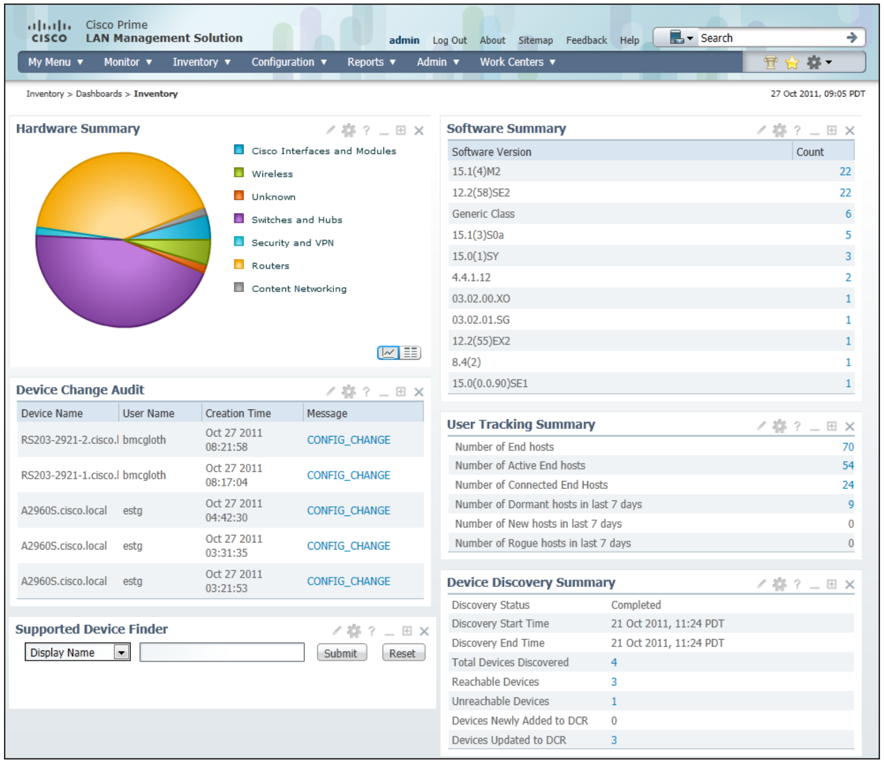
Installation and Deployment

Most often, network administrators are unsure of the most efficient method to configure Cisco LMS. Cisco LMS provides a very important feature: the Getting Started workflow. This guided sequence eliminates configuration guesswork and assists you in performing essential and optional configuration and management tasks. It is a quick and sure way of getting Cisco LMS running with minimal human errors.

Configuration and Inventory Management

As enterprise networks grow, network administrators have a tedious job in keeping track of devices being added or removed. Administrators also have to ensure that the devices are running proper software and that configurations are archived. And they must implement network compliance by enforcing policies across the network. This is where the configuration and inventory management function of Cisco LMS plays an important role. Resource Manager Essentials contains a set of automated features to help IT staff with configuration and inventory management:

Figure 2 - Inventory Dashboard



Hardware Summary

Software Summary

Software Version	Count
15.1(4)M2	22
12.2(58)SE2	22
Generic Class	6
15.1(3)S0a	5
15.0(1)SY	3
4.4.1.12	2
03.02.00.XO	1
03.02.01.SG	1
12.2(55)EX2	1
8.4(2)	1
15.0(0.0.90)SE1	1

Device Change Audit

Device Name	User Name	Creation Time	Message
RS203-2921-2.cisco.l	bmcgloth	Oct 27 2011 08:21:58	CONFIG_CHANGE
RS203-2921-1.cisco.l	bmcgloth	Oct 27 2011 08:17:04	CONFIG_CHANGE
A2960S.cisco.local	estg	Oct 27 2011 04:42:30	CONFIG_CHANGE
A2960S.cisco.local	estg	Oct 27 2011 03:31:35	CONFIG_CHANGE
A2960S.cisco.local	estg	Oct 27 2011 03:21:53	CONFIG_CHANGE

User Tracking Summary

Number of End hosts	70
Number of Active End hosts	54
Number of Connected End Hosts	24
Number of Dormant hosts in last 7 days	9
Number of New hosts in last 7 days	0
Number of Rogue hosts in last 7 days	0

Supported Device Finder

Device Discovery Summary

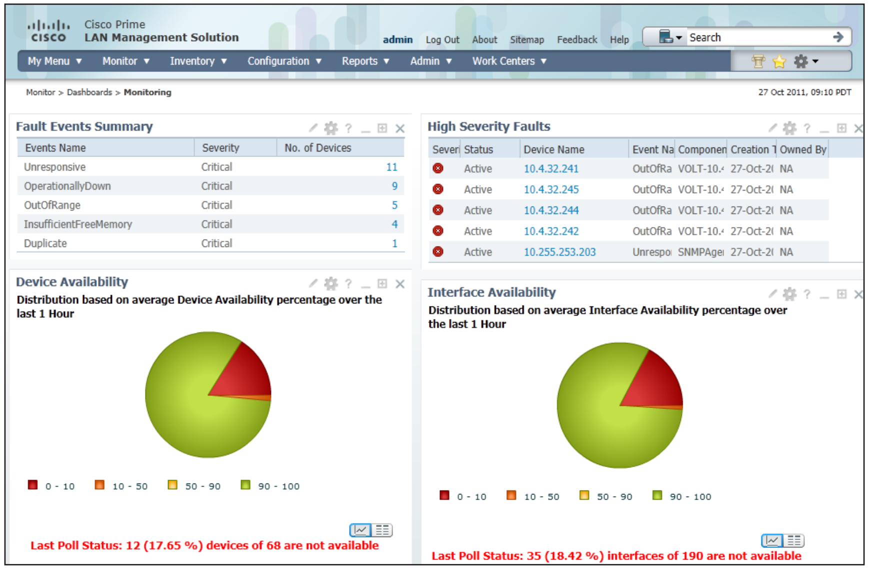
Discovery Status	Completed
Discovery Start Time	21 Oct 2011, 11:24 PDT
Discovery End Time	21 Oct 2011, 11:24 PDT
Total Devices Discovered	4
Reachable Devices	3
Unreachable Devices	1
Devices Newly Added to DCR	0
Devices Updated to DCR	3

- Inventory Manager—Builds and maintains an up-to-date software and hardware inventory, providing a detailed inventory report, which you can customize, or a predefined inventory.
- Configuration Manager—Maintains an active archive of multiple iterations of configuration files for every managed device and simplifies the deployment of configuration changes. ConfigEditor is a utility to change, compare and deploy configurations on one device. NetConfig is a similar utility to perform such tasks on multiple devices.
- Software Manager—Simplifies and speeds up software image analysis and deployment. This feature helps in automatic upgrade analysis and helps to select the right image. A network administrator can also use this feature to import images, stage images (local or remote), and then install them on a single device or group of devices.
- Syslog Analysis—Collects and analyzes syslog messages to help isolate network error conditions. A network administrator can filter syslog messages and designate an action based on the messages.
- Audit Service—Continuously monitors incoming data versus stored data to provide comprehensive reports on software image, inventory and configuration changes. It also tracks the changes made to Cisco LMS by the system administrator.
- Compliance Management—Provides a way to enforce certain policies (or configurations) to ensure that the network is compliant per internal or government regulations.

Monitoring and Fault Management

Two of a network administrator's most important tasks are to ensure high network-availability and resolve any network issues as they occur. Cisco LMS provides both monitoring and fault management functionalities, using Simple Network Management Protocol (SNMP) polling and traps. The Cisco LMS auto-monitoring feature proactively monitors the network for any indication of device or network fault, enabling quick network repair turnaround time with minimum service degradation.

Figure 3 - Monitoring Dashboard



Fault Events Summary

Events Name	Severity	No. of Devices
Unresponsive	Critical	11
OperationallyDown	Critical	9
OutOfRange	Critical	5
InsufficientFreeMemory	Critical	4
Duplicate	Critical	1

High Severity Faults

Severi	Status	Device Name	Event Na	Componen	Creation T	Owned By
●	Active	10.4.32.241	OutOfRa	VOLT-10.	27-Oct-20	NA
●	Active	10.4.32.245	OutOfRa	VOLT-10.	27-Oct-20	NA
●	Active	10.4.32.244	OutOfRa	VOLT-10.	27-Oct-20	NA
●	Active	10.4.32.242	OutOfRa	VOLT-10.	27-Oct-20	NA
●	Active	10.255.253.203	Unrespo	SNMPAge	27-Oct-20	NA

Distribution based on average Device Availability percentage over the last 1 Hour

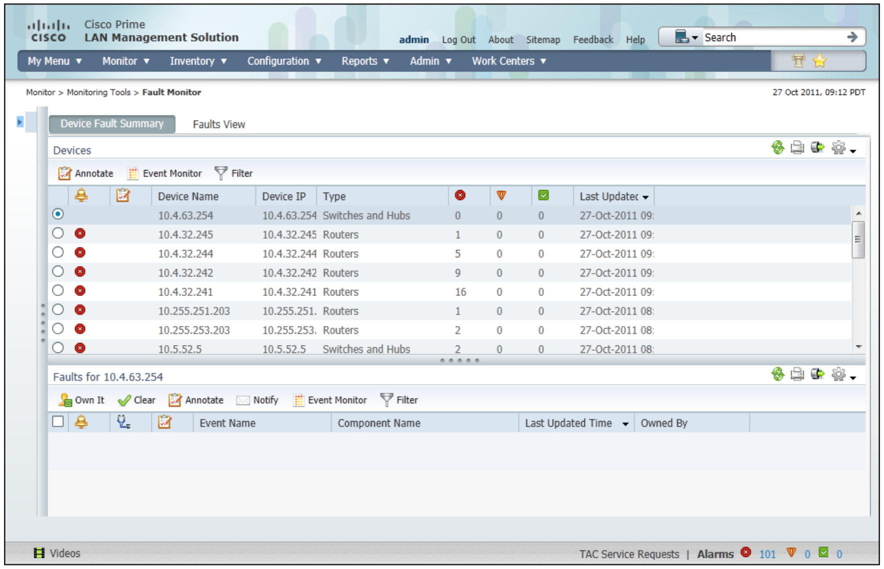
Last Poll Status: 12 (17.65 %) devices of 68 are not available

Distribution based on average Interface Availability percentage over the last 1 Hour

Last Poll Status: 35 (18.42 %) interfaces of 190 are not available

Cisco LMS Fault Monitor is a centralized browser where administrators can read, in a single view, information on faults and events. Fault Monitor collects information about faults from all devices in real time and can display it for single devices or groups. After administrators have acted on a fault, they can clear the alarms, as well.

Figure 4 - Fault Monitor Dashboard



			Device Name	Device IP	Type	⊗	▽	✓	Last Updatec ▼
●			10.4.63.254	10.4.63.254	Switches and Hubs	0	0	0	27-Oct-2011 09:
○	⊗		10.4.32.245	10.4.32.245	Routers	1	0	0	27-Oct-2011 09:
○	⊗		10.4.32.244	10.4.32.244	Routers	5	0	0	27-Oct-2011 09:
○	⊗		10.4.32.242	10.4.32.242	Routers	9	0	0	27-Oct-2011 09:
○	⊗		10.4.32.241	10.4.32.241	Routers	16	0	0	27-Oct-2011 09:
○	⊗		10.255.251.203	10.255.251.	Routers	1	0	0	27-Oct-2011 08:
○	⊗		10.255.253.203	10.255.253.	Routers	2	0	0	27-Oct-2011 08:
○	⊗		10.5.52.5	10.5.52.5	Switches and Hubs	2	0	0	27-Oct-2011 08:

□				Event Name	Component Name	Last Updated Time ▼	Owned By

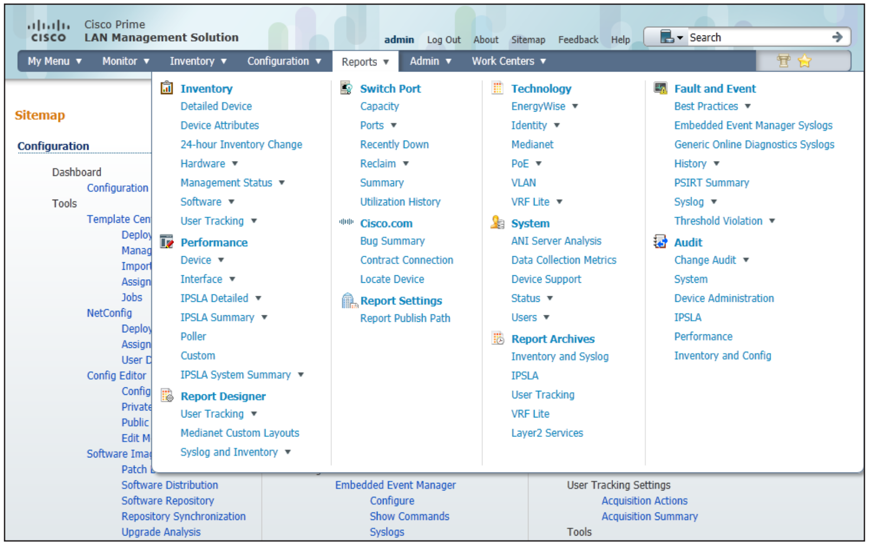
Templates

Most of the time, administrators have to deploy configurations that are global to the network (switch configurations, permissions, etc.), and they spend a fair amount of time propagating these configurations manually on a device-by-device basis. Cisco LMS provides the Template Center feature, which can greatly reduce the configuration deployment time by using predefined or customized templates. These templates can also be imported from machines and then stored as system-defined templates in Cisco LMS.

Reporting

Cisco LMS provides a single launch point for all the reports—including inventory, switch ports, technology, fault and event, performance, and audit reports. Administrators can archive these reports and view them at a later time.

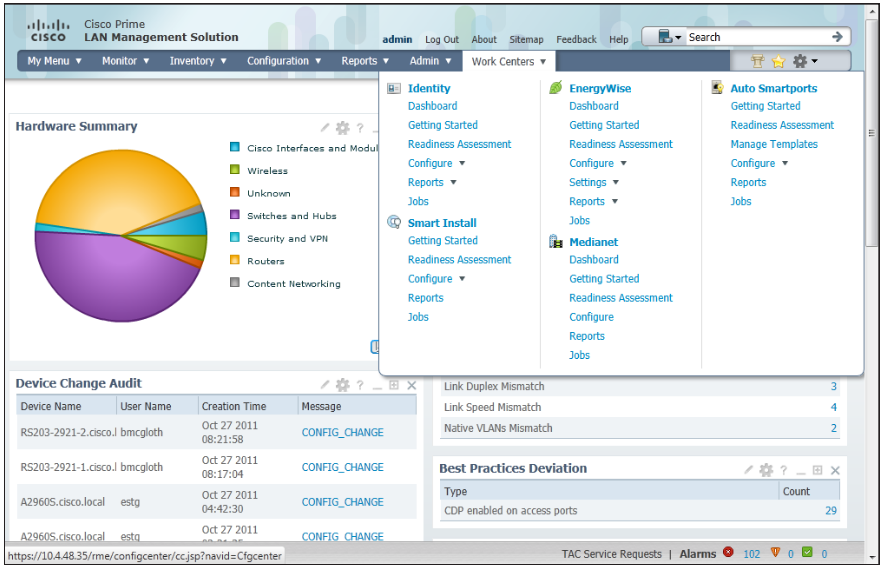
Figure 5 - Report Generation and View Layout



Work Centers

The Work Centers feature allows administrators to access more advanced features (such as EnergyWise, Smart Install, Identity, and Auto Smart ports) for day 1 to day N operations.

Figure 6 - Work Center Layout



Device Change Audit

Device Name	User Name	Creation Time	Message
RS203-2921-2.cisco.l	bmcgloth	Oct 27 2011 08:21:58	CONFIG_CHANGE
RS203-2921-1.cisco.l	bmcgloth	Oct 27 2011 08:17:04	CONFIG_CHANGE
A2960S.cisco.local	estg	Oct 27 2011 04:42:30	CONFIG_CHANGE
A2960S.cisco.local	estg	Oct 27 2011	CONFIG_CHANGE

Link Duplex Mismatch	3
Link Speed Mismatch	4
Native VLANs Mismatch	2

Best Practices Deviation

Type	Count
CDP enabled on access ports	29

https://10.4.48.35/rme/configcenter/cc.jsp?navid=Cfgcenter

TAC Service Requests | Alarms 102 0 0

Notes

Deployment Details

Process

Installing and Configuring Cisco LMS

1. Obtain a license
2. Install software
3. Configure basic settings
4. Configure Cisco LMS user authentication
5. Configure Cisco LMS user roles
6. Add devices
7. Manage administrator tasks
8. Configure syslog collection

Procedure 1 Obtain a license

Cisco LMS offers a single software installation that can manage up to 10,000 devices. Software licensing allows an organization to evaluate the software and before deciding how you want to proceed: purchasing the license, piloting a small deployment before rolling out organization-wide, or growing your network management system along with your network. Licensing allows you to first evaluate the software without requiring that you reinstall the software later.

There are two ways to acquire a license:

- **Physical media**—Ordering the product DVD that comes with a Product Activation Key (PAK). The PAK is normally printed on the software claim certificate included with product DVD kit. Use the PAK on http://cisco.com/go/license in order to get the license.
- **Downloading Cisco LMS evaluation software and ordering a digital PAK**—Download an evaluation copy of Cisco LMS from http://cisco.com/go/nmsevals. You will receive a PAK via email. Use this PAK on http://cisco.com/go/license in order to get the license.

Procedure 2 Install software

You can install the Cisco LMS soft appliance using the LMS 4.1 OVA image from the Cisco LMS 4.1 DVD. Before installing, please take note that:

- Make sure that your system meets the recommended hardware and software specifications listed in the release notes.
- It takes from approximately 30 minutes (deployment in the local system) or 50 minutes (deployment in the network) to install the soft appliance on a virtualized environment.
- Soft appliance OVA software can be installed only in the VMware environment.

Reader Tip

You need not install any soft appliance image on the VM before installing Cisco LMS 4.1, because the LMS 4.1 OVA image has an embedded RedHat Enterprise soft appliance.

Recommendations before installation:

- Configure DNS entries for each network device.
- Enable SNMP and Secure Shell (SSH) Protocol on the devices you are going to import.

Step 1: You must first install and power on the Cisco LMS OVA on the VMware ESX/ESXi server using vSphere.

The Welcome screen appears.

Step 2: Press **Enter** in the console window to continue with the next step.

Step 3: Enter the following configuration details of the server:

- Hostname—**LMS**
- IP Address—**10.10.48.35**
- IP Netmask—**255.255.255.0**
- Default Gateway—**10.10.48.1**
- DNS Domain Name—**cisco.local**
- Primary Name Server—**10.10.48.10**
- Primary NTP Server—**10.10.48.17**
- System Time Zone—**America/Los_Angeles**

Step 4: Enter the username to access the Cisco LMS appliance console. This user will have the privilege to enable the shell access. The default username is *sysadmin*. You cannot use *root* as the username because it is a reserved username. You can use only alphanumeric characters for the username.

Step 5: Enter and confirm the sysadmin password. By default, this password will be set as the shell password.

Step 6: Enter and confirm the password for the admin account to use to log into Cisco LMS using the browser. This password must contain a minimum of five characters and will also be used for the System Identity account.

The following message appears:

> For security reasons, passwords are not displayed. Do you want to view all the passwords? (Y/N) [N]:

Step 7: Enter **N**.

It will take 15 to 20 minutes to process the database engine.

The server will be automatically rebooted.

Procedure 3 Configure basic settings

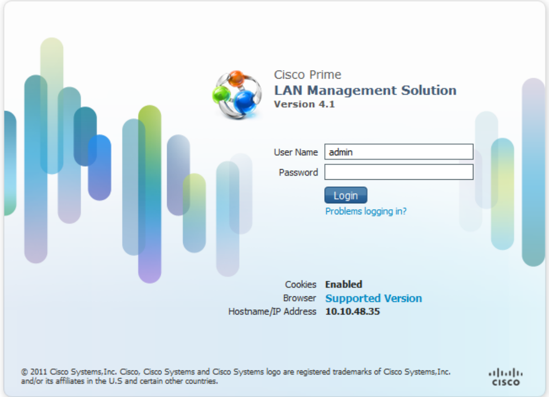
Step 1: On the client machine's web browser, disable any pop-up blockers and ensure that JavaScript is enabled.

To enable JavaScript:

- In Internet Explorer 4.x or later, navigate to **Tools > Internet Options > Security > Custom level > Settings**, and then under **Scripting of Java applets**, select **Enable**.
- In Firefox, navigate to **Tools > Option > Content**, and then select the **Enable JavaScript** check box.

Step 2: Open the Cisco LMS portal in your web browser. The browser reaches the Cisco LMS portal by appending the port number 1741 to the DNS host name or IP address of the server on which you installed Cisco LMS (example: http://10.10.48.35:1741).

Step 3: Log in using the username admin and the password that you provided during installation.



User Name: admin
Password:

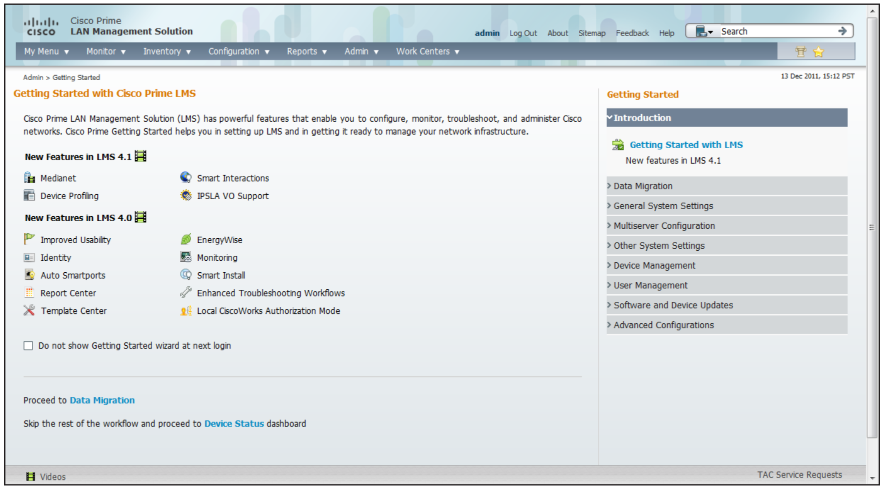
Cookies: Enabled
Browser: Supported Version
Hostname/IP Address: 10.10.48.35

© 2011 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries.

Step 4: The Getting Started pane shows you the workflow for configuring Cisco LMS.

Tech Tip

The configuration process described in this guide will not use every step in the Getting Started workflow.



Getting Started with Cisco Prime LMS

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

New Features in LMS 4.1

Medianet	Smart Interactions
Device Profiling	IPSLA VO Support

New Features in LMS 4.0

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

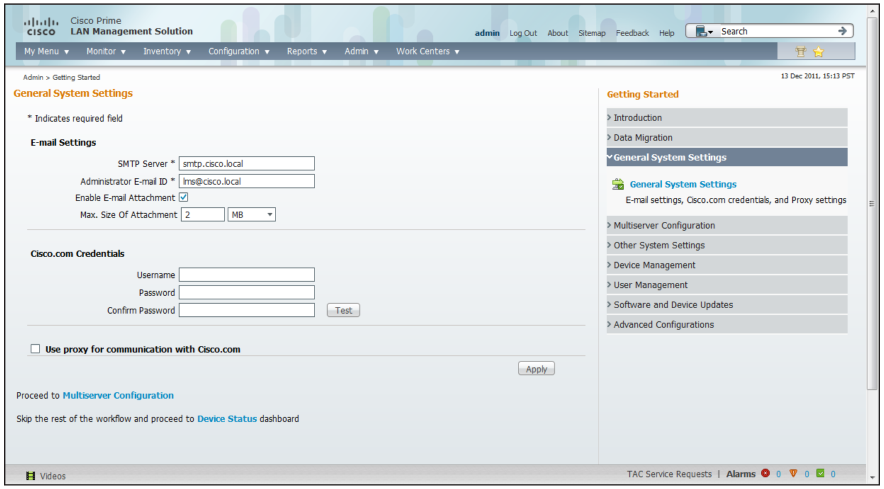
□ Do not show Getting Started wizard at next login

Proceed to Data Migration

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

Getting Started with LMS
New features in LMS 4.1

Step 5: To receive automatic email alerts (about network issues, job status, report generation, etc.), click **General System Settings**, enter values in the **SMTP Server** and **Administrator E-mail ID** fields, and then click **Apply**.



General System Settings

* Indicates required field

E-mail Settings

SMTP Server * smtp.cisco.local
Administrator E-mail ID * lms@cisco.local
Enable E-mail Attachment ☑
Max. Size Of Attachment 2 MB

Cisco.com Credentials

Username
Password
Confirm Password

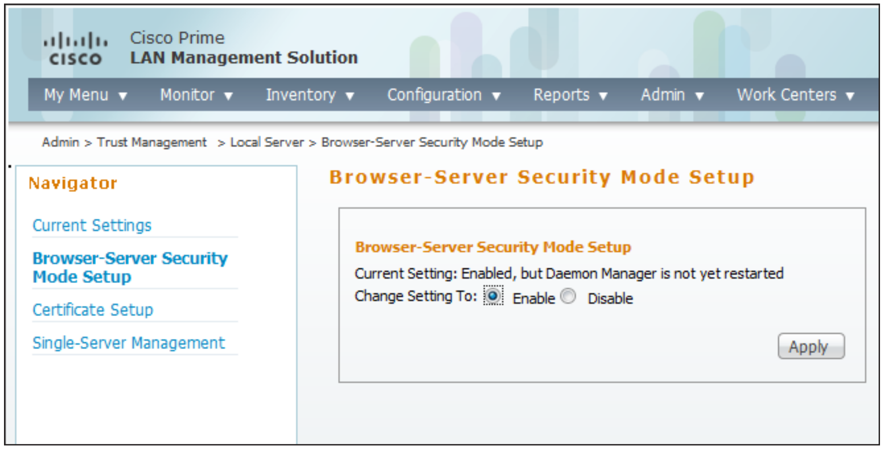
□ Use proxy for communication with Cisco.com

Proceed to Multiserver Configuration

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

General System Settings
E-mail settings, Cisco.com credentials, and Proxy settings

Step 6: To configure the Cisco LMS portal to support HTTPS connections, navigate to **Admin > Trust Management > Local Server > Browser-Server Security Mode Setup**.



Browser-Server Security Mode Setup

Browser-Server Security Mode Setup

Current Setting: Enabled, but Daemon Manager is not yet restarted

Change Setting To: ● Enable ○ Disable

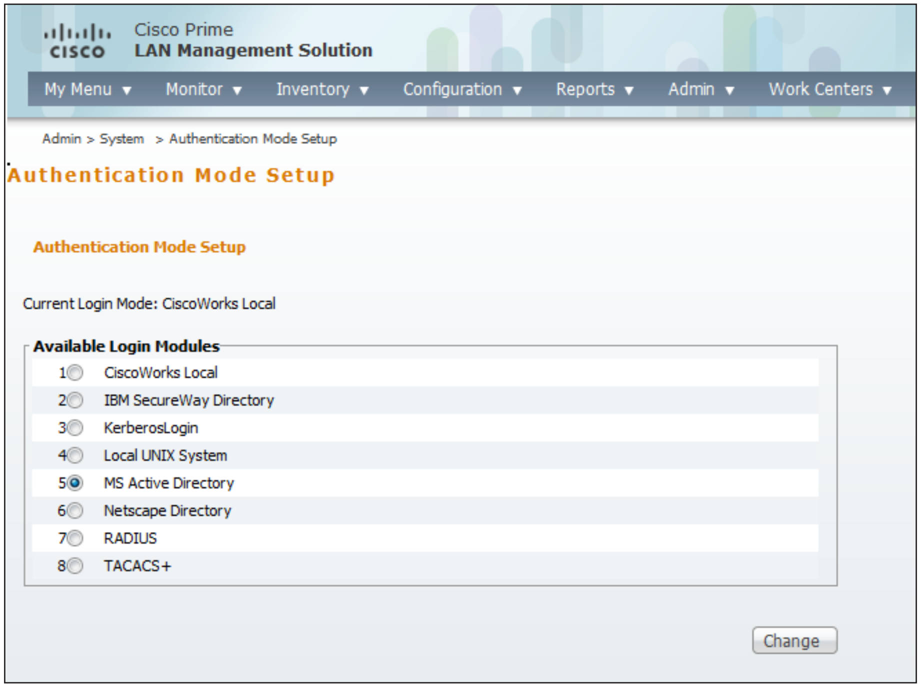
Step 7: Select **Enable**, and then click **Apply**.

Procedure 4 Configure Cisco LMS user authentication

Cisco LMS can use its local database, Active Directory, Lightweight Directory Access Protocol (LDAP), TACACS+, and many other modules to authenticate user logins. Cisco SBA for Midsize Organizations uses Active Directory, when available, for centralized authentication. To enable a common authentication experience for network administrators across network devices and the network management system, this guide describes how to configure Cisco LMS to use Active Directory authentication.

Step 1: Click **Admin > System > Authentication Mode Setup**.

Step 2: Select **MS Active Directory**, and then click **Change**.



Admin > System > Authentication Mode Setup

Authentication Mode Setup

Authentication Mode Setup

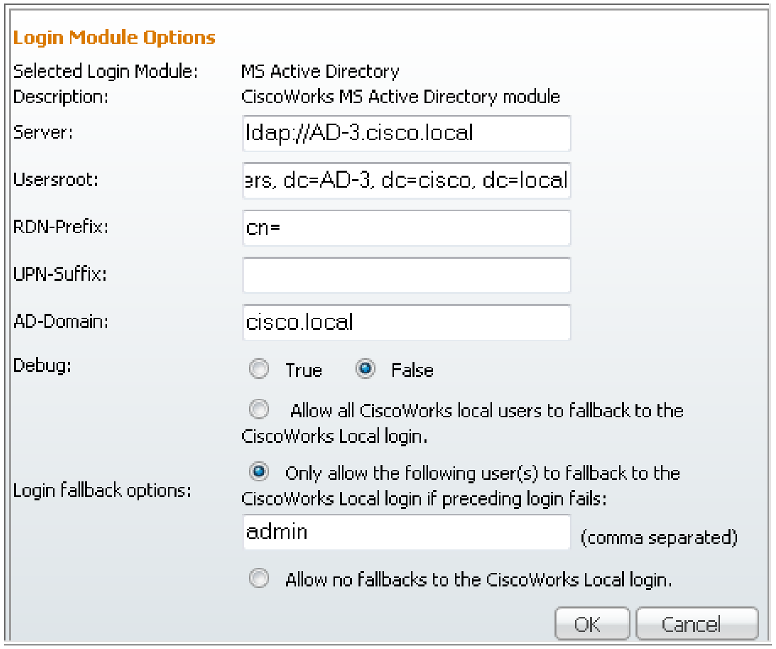
Current Login Mode: CiscoWorks Local

Available Login Modules

1 ○ CiscoWorks Local
2 ○ IBM SecureWay Directory
3 ○ KerberosLogin
4 ○ Local UNIX System
5 ● MS Active Directory
6 ○ Netscape Directory
7 ○ RADIUS
8 ○ TACACS+

Change

Step 3: Set the **Server** (for example, ldap://AD-3.cisco.local), the **Usersroot** directory path(for example, cn=users, dc=AD-3, dc=cisco, dc=local), and **AD-Domain** (for example, cisco.local), and then click **OK**.



Login Module Options

Selected Login Module: MS Active Directory
Description: CiscoWorks MS Active Directory module
Server: ldap://AD-3.cisco.local
Usersroot: ers, dc=AD-3, dc=cisco, dc=local
RDN-Prefix: cn=
UPN-Suffix:
AD-Domain: cisco.local
Debug: ○ True ● False

Login fallback options:
○ Allow all CiscoWorks local users to fallback to the CiscoWorks Local login.
● Only allow the following user(s) to fallback to the CiscoWorks Local login if preceding login fails:
admin (comma separated)
○ Allow no fallbacks to the CiscoWorks Local login.

OK Cancel

Step 4: When the Login Module Change Summary window appears, saying the changes were updated successfully, click **OK.**

Procedure 5 Configure Cisco LMS user roles

A role is a collection of privileges that dictates the type of system access the user has. The predefined roles are:

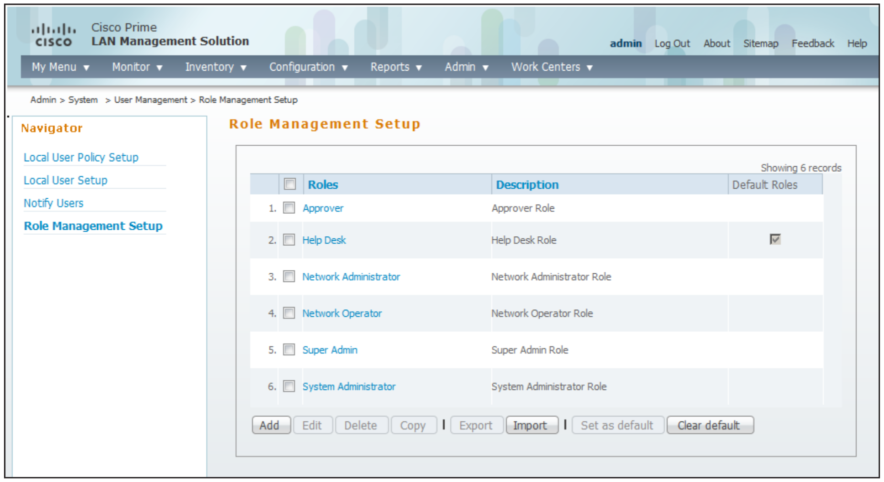
- Help Desk—These users can access network status information only. They cannot perform any action on a device or schedule a job on a network.
- Network Operator—Users can perform all Help Desk tasks and tasks related to network data collection. They cannot perform any task that requires write-access on the network.
- Approver—Users can approve all tasks.
- Network Administrator—Users can perform all Network Operator tasks, as well as configuration changes.
- System Administrator—Users can perform all Cisco LMS system administration tasks.
- Super Admin—Users can perform all Cisco LMS operations, including administration and approval tasks.

When using an authentication module other than the Cisco LMS local database, Cisco LMS authenticates the user against the external module., After the user is successfully authenticated, Cisco LMS will assign the default role to this user unless there is a pre-assigned role for this user.

Step 1: Navigate to **Admin > System > User Management > Role Management Setup**.

Step 2: Select the check box next to the role you want to define as the default role, and then click **Set as default**.

Choose the role that you will assign to the majority of users in your organization. For example, if the majority of users should be able to access Cisco LMS to review network configuration and performance, but not apply any changes to Cisco LMS or the network, leave Help Desk as the default role.



Admin > System > User Management > Role Management Setup

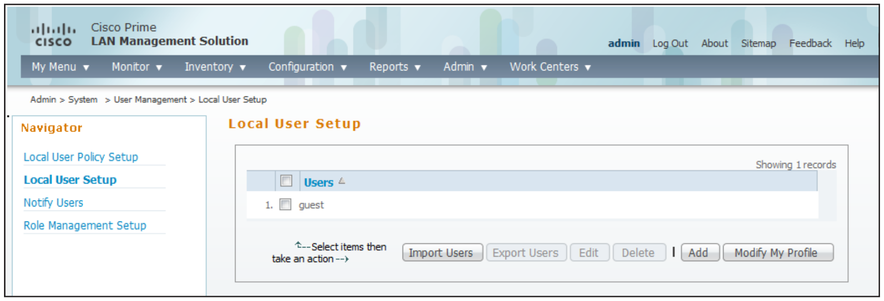
Role Management Setup

Showing 6 records

	□	Roles	Description	Default Roles
1.	□	Approver	Approver Role	
2.	□	Help Desk	Help Desk Role	☑
3.	□	Network Administrator	Network Administrator Role	
4.	□	Network Operator	Network Operator Role	
5.	□	Super Admin	Super Admin Role	
6.	□	System Administrator	System Administrator Role	

Step 3: For any users who require different permissions than those included in the default role, create local user accounts. You will assign a Cisco LMS role to each of the local user accounts you create.

Step 4: Navigate to **Admin > System > User Management > Local User Setup**.



Admin > System > User Management > Local User Setup

Local User Setup

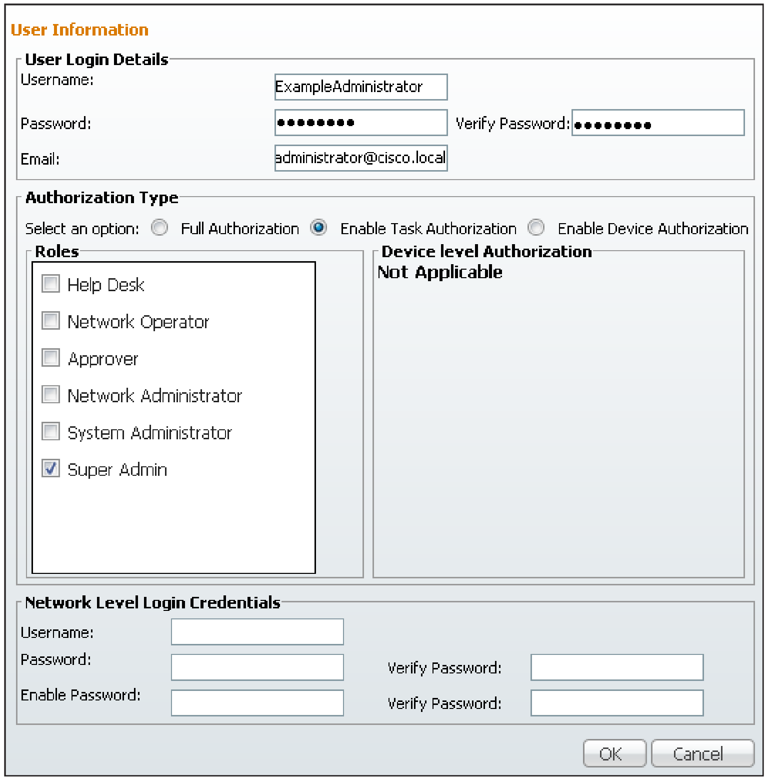
Showing 1 records

	□	Users
1.	□	guest

↑--Select items then take an action -->

Step 5: Click **Add**. The Add Users window opens.

Step 6: Enter the username used in the Active Directory login, configure a password (it does not have to match the Active Directory login password and it will not be used during authentication), select the **Super Admin** check box, and then click **OK**.



User Information

User Login Details

Username: ExampleAdministrator

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

Email: administrator@cisco.local

Authorization Type

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

Roles

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

Device level Authorization

Not Applicable

Network Level Login Credentials

Username:

Password: Verify Password:

Enable Password: Verify Password:

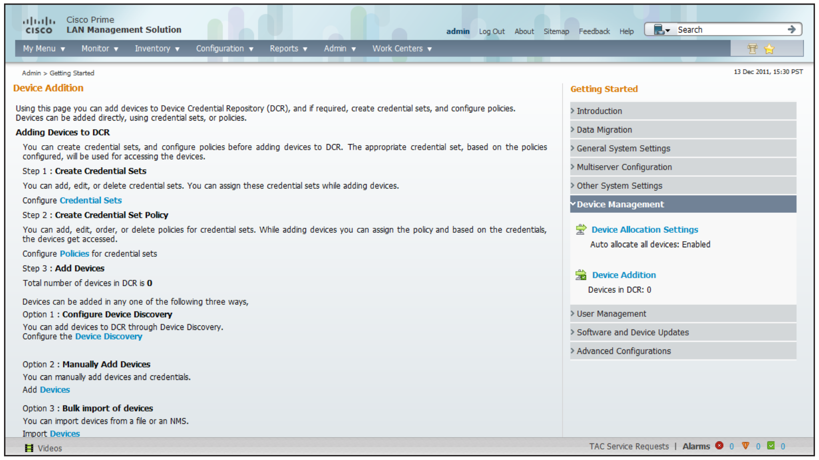
Procedure 6 Add devices

Before Cisco LMS can manage a device, the device must be in the LMS Device Credential Repository (DCR). You can add devices to the DCR in two ways:

- Discover the devices using a discovery protocol
- Add devices manually

Cisco LMS supports layer 2 and layer 3 protocols for device discovery. Device discovery using Cisco Discovery Protocol is the preferred protocol used by Cisco LMS to discover network devices in the LAN. Both Cisco Discovery Protocol and SNMP must be enabled on devices before you can use this procedure.

Step 1: To begin configuration, navigate to **Admin > Getting Started > Device Management > Device Addition**.



Device Addition

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

Adding Devices to DCR

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

Step 1 : **Create Credential Sets**

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

Configure Credential Sets

Step 2 : **Create Credential Set Policy**

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

Configure Policies for credential sets

Step 3 : **Add Devices**

Total number of devices in DCR is **0**

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

Option 1 : **Configure Device Discovery**

You can add devices to DCR through Device Discovery.
Configure the Device Discovery

Option 2 : **Manually Add Devices**

You can manually add devices and credentials.

Add Devices

Option 3 : **Bulk import of devices**

You can import devices from a file or an NMS.

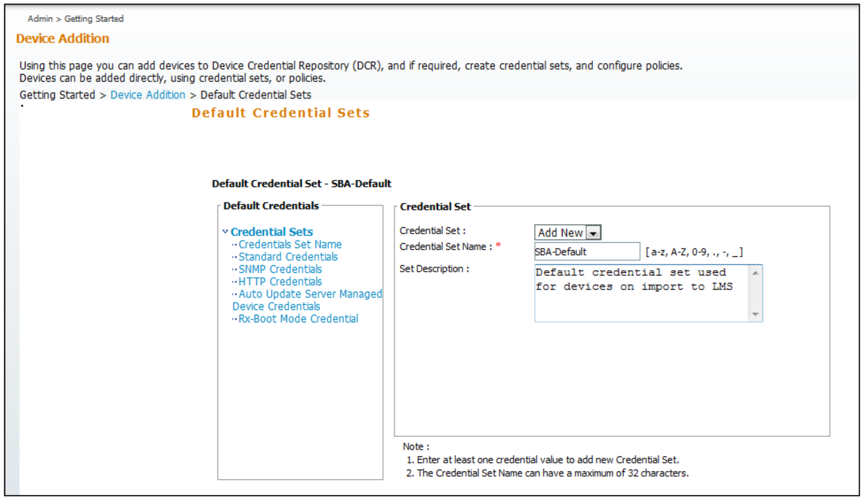
Import Devices

Getting Started

- Introduction
- Data Migration
- General System Settings
- Multiserver Configuration
- Other System Settings
- Device Management
  - Device Allocation Settings
    Auto allocate all devices: Enabled
  - Device Addition
    Devices in DCR: 0
- User Management
- Software and Device Updates
- Advanced Configurations

Step 2: Click **Credential Sets**. Credential sets allow Cisco LMS to apply a default set of credentials to devices after discovery. Cisco LMS then uses the credentials in order to manage the device inventory, configuration, and software.

Step 3: Click **Credential Set Name**, and then set the **Credential Set Name** to **SBA-Default**.



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

Getting Started > Device Addition > Default Credential Sets

Default Credential Sets

Default Credential Set - SBA-Default

Credential Set

Credential Set : Add New

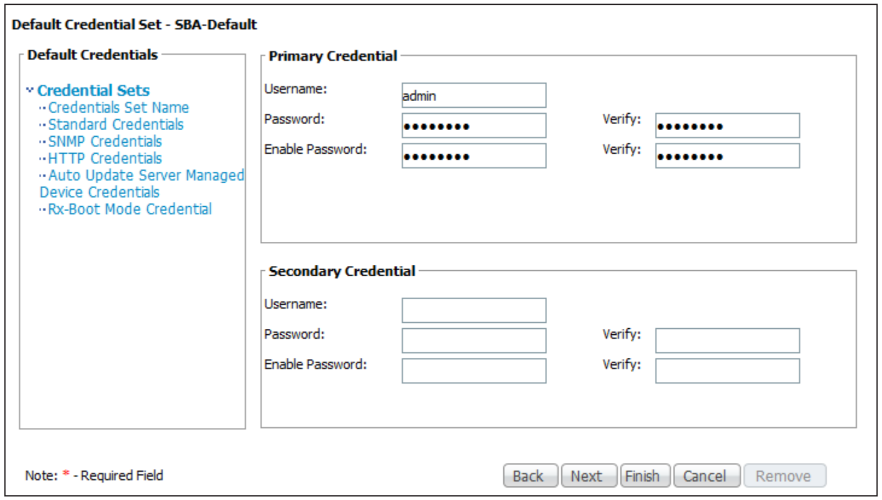
Credential Set Name : * SBA-Default [a-z, A-Z, 0-9, ., -, _]

Set Description : Default credential set used for devices on import to LMS

Note :

1. Enter at least one credential value to add new Credential Set.
2. The Credential Set Name can have a maximum of 32 characters.

Step 4: Click **Standard Credentials**, and then enter the **Username** (example: admin), **Password**, and **Enable Password** that Cisco LMS should use when logging in via SSH.


Default Credential Set - SBA-Default

Primary Credential

Username: admin

Password: •••••••• Verify: ••••••••

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

Secondary Credential

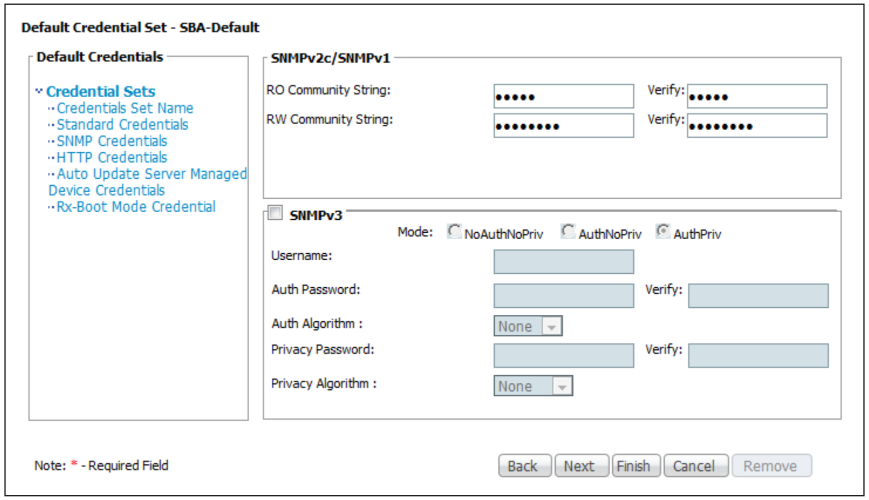
Username:

Password: Verify:

Enable Password: Verify:

Note: * - Required Field

Step 5: Click **SNMP Credentials**, and then configure the RO Community String (cisco) and RW Community String (cisco123) that Cisco LMS should use to poll the network devices.


Default Credential Set - SBA-Default

SNMPv2c/SNMPv1

RO Community String: ••••• Verify: •••••

RW Community String: •••••••• Verify: ••••••••

□ SNMPv3

Mode: ○ NoAuthNoPriv ○ AuthNoPriv ● AuthPriv

Username:

Auth Password: Verify:

Auth Algorithm : None

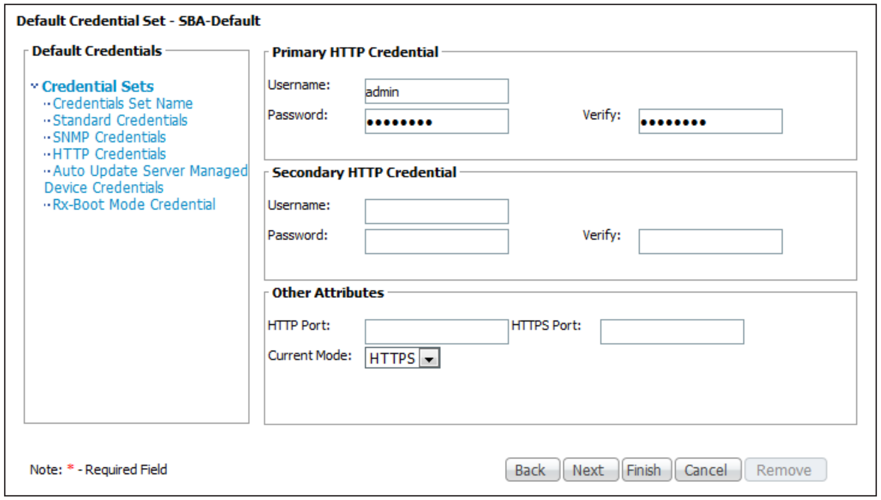
Privacy Password: Verify:

Privacy Algorithm : None

Note: * - Required Field

Step 6: Click **HTTP Credentials**, and then configure the **Username** (admin) and **Password** that Cisco LMS should use when configuring a device via HTTPS.

Step 7: From the **Current Mode** drop-down list, choose **HTTPS**., and then click **Finish**.


Default Credential Set - SBA-Default

Primary HTTP Credential

Username: admin

Password: •••••••• Verify: ••••••••

Secondary HTTP Credential

Username:

Password: Verify:

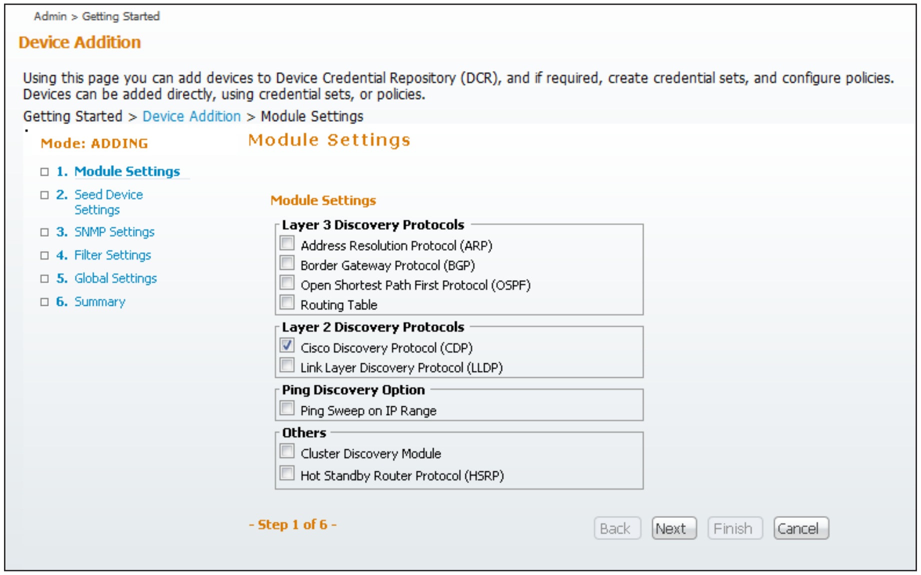
Other Attributes

HTTP Port: HTTPS Port:

Current Mode: HTTPS

Note: * - Required Field

Step 8: Navigate to **Admin > Getting Started**, and then click **Device Discovery**. The Module Settings pane appears. You use this pane to enable the discovery protocol(s) that Cisco LMS will use to discover the devices on the network. Select the **Cisco Discovery Protocol** check box, and then click **Next**.



Admin > Getting Started

Device Addition

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

Getting Started > Device Addition > Module Settings

Mode: ADDING

Module Settings

Module Settings

Layer 3 Discovery Protocols
- ☐ Address Resolution Protocol (ARP)
- ☐ Border Gateway Protocol (BGP)
- ☐ Open Shortest Path First Protocol (OSPF)
- ☐ Routing Table

Layer 2 Discovery Protocols
- ☑ Cisco Discovery Protocol (CDP)
- ☐ Link Layer Discovery Protocol (LLDP)

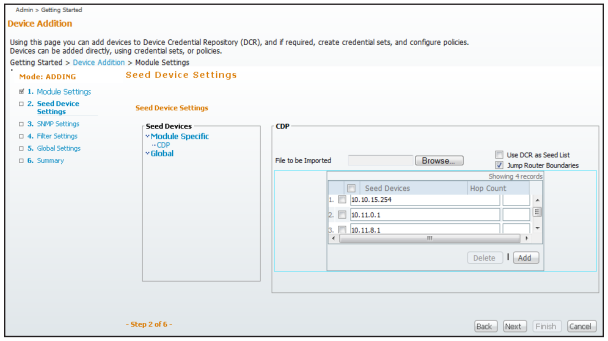
Ping Discovery Option
- ☐ Ping Sweep on IP Range

Others
- ☐ Cluster Discovery Module
- ☐ Hot Standby Router Protocol (HSRP)

- Step 1 of 6 -

Step 9: The seed device setting page appears. A seed device is the start point from which Cisco LMS discovers the network. The seed devices should be the core devices on the network and any device does that share layer-2 adjacency to the headquarters network. In Cisco SBA Borderless Networks for Midsize Organizations, the LAN core switch will be a Cisco Catalyst 3750-X Series switch stack, a Catalyst 4507 chassis-based switch with a Supervisor 7, or a Catalyst 6500 Virtual Switching System pair, depending on your scale and performance requirements.

Click **CDP**, click **Add**, and then configure the first seed device as the core switch. Click **Add** again, configure the loopback addresses of WAN routers at remote sites, and then click **Next**.



Admin > Getting Started

Device Addition

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

Getting Started > Device Addition > Module Settings

Mode: ADDING

Seed Device Settings

Seed Device Settings

CDP

File to be Imported

☐ Use DCR as Seed List

☑ Jump Router Boundaries

Showing 4 records

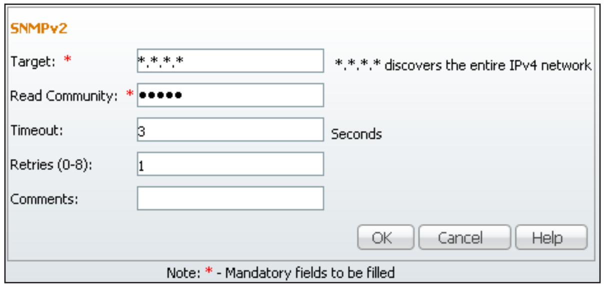
	☐	Seed Devices	Hop Count
1.	☐	10.10.15.254	
2.	☐	10.11.0.1	
3.	☐	10.11.8.1	

- Step 2 of 6 -

Step 10: On the SNMP settings configuration page, click **Add**.

Step 11: A new window pops up. Enter the target value (*.*.*.*), which tells Cisco LMS to use this SNMP community string for all devices during discovery.

Step 12: Enter the read-only SNMP community string configured on your network devices (cisco), and then click **OK**.



SNMPv2

Target: * *.*.*.*   *.*.*.* discovers the entire IPv4 network

Read Community: * •••••

Timeout: 3 Seconds

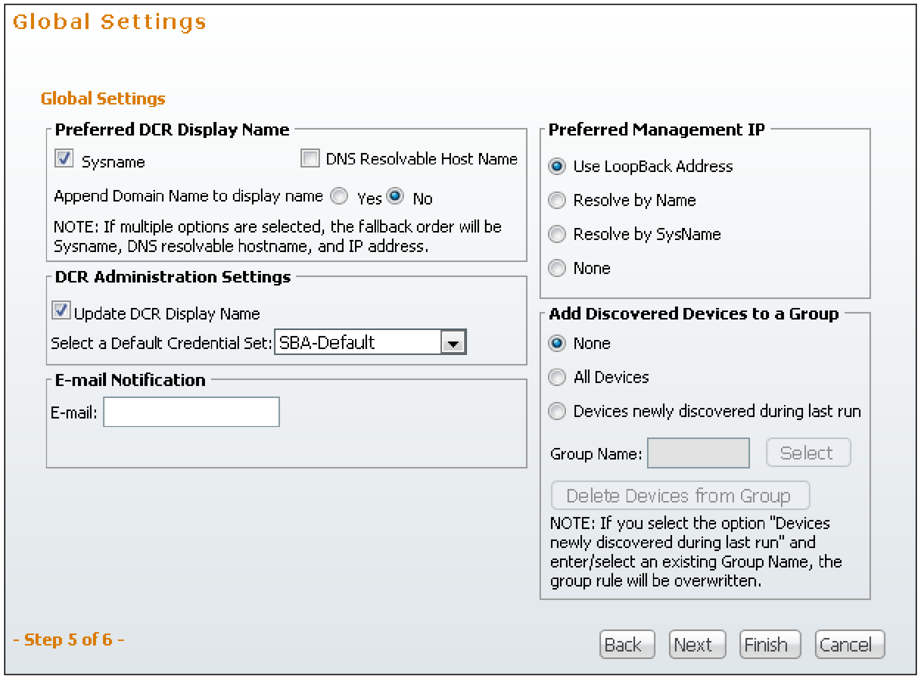
Retries (0-8): 1

Comments:

Note: * - Mandatory fields to be filled

Step 13: Click **Next** twice to reach the Global Settings page, and then configure these settings:

- Under Preferred DCR Display Name, select **Sysname**, and then clear the checkbox next to **DNS Resolvable Host Name**.
- Under DCR Administration Settings, select the **Update DCR Display Name** check box.
- In the **Default Credential Set** drop-down list, choose **SBA-Default**.
- Under Preferred Management IP, select **Use LoopBack Address**, and then click **Finish**.



Global Settings

Global Settings

Preferred DCR Display Name

☑ Sysname ☐ DNS Resolvable Host Name

Append Domain Name to display name ○ Yes ● No

NOTE: If multiple options are selected, the fallback order will be Sysname, DNS resolvable hostname, and IP address.

DCR Administration Settings

☑ Update DCR Display Name

Select a Default Credential Set: SBA-Default

E-mail Notification

E-mail:

Preferred Management IP

● Use LoopBack Address

○ Resolve by Name

○ Resolve by SysName

○ None

Add Discovered Devices to a Group

● None

○ All Devices

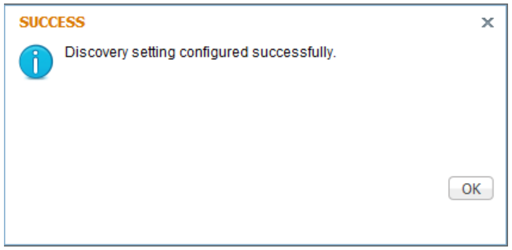
○ Devices newly discovered during last run

Group Name:

NOTE: If you select the option "Devices newly discovered during last run" and enter/select an existing Group Name, the group rule will be overwritten.

- Step 5 of 6 -

Step 14: In the message that informs you that discovery settings are successfully configured, click **OK**.

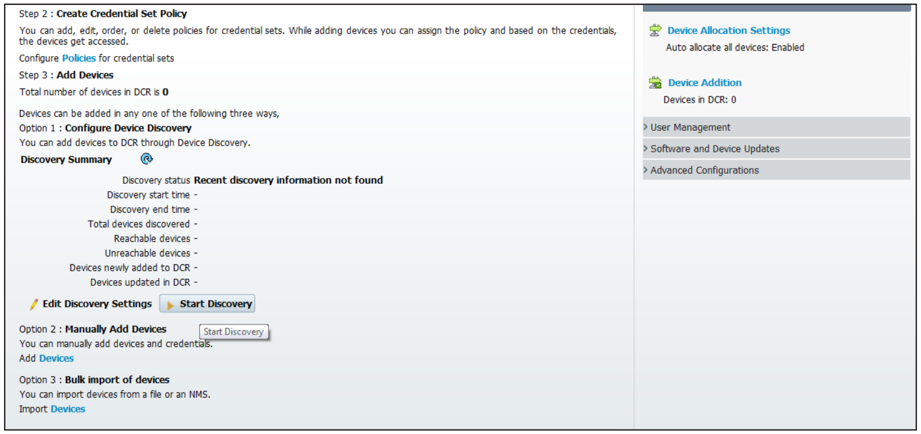


SUCCESS

Discovery setting configured successfully.

Step 15: Near the bottom of the Adding Devices to DCR page, click **Start Discovery**.

Cisco LMS starts discovering the devices on the network. The amount of time this discovery process will take depends on the number of devices on the network. The Discovery window will be refreshed every 5 seconds and will update the number of devices being discovered.



Step 2 : **Create Credential Set Policy**

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

Configure Policies for credential sets

Step 3 : **Add Devices**

Total number of devices in DCR is **0**

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

Option 1 : **Configure Device Discovery**

You can add devices to DCR through Device Discovery.

Discovery Summary

Discovery status **Recent discovery information not found**
Discovery start time -
Discovery end time -
Total devices discovered -
Reachable devices -
Unreachable devices -
Devices newly added to DCR -
Devices updated in DCR -

Option 2 : **Manually Add Devices**

You can manually add devices and credentials.

Add Devices

Option 3 : **Bulk import of devices**

You can import devices from a file or an NMS.

Import Devices

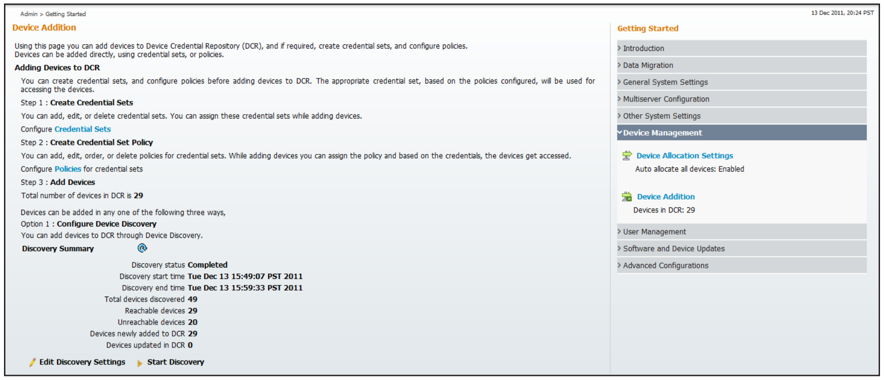
Device Allocation Settings

Auto allocate all devices: Enabled

Device Addition

Devices in DCR: 0

After the process is completed, the status will change from running to complete.



Admin > Getting Started

13 Dec 2011, 20:24 PST

Device Addition

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

Adding Devices to DCR

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

Step 1 : **Create Credential Sets**

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

Configure Credential Sets

Step 2 : **Create Credential Set Policy**

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

Configure Policies for credential sets

Step 3 : **Add Devices**

Total number of devices in DCR is **29**

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

Option 1 : **Configure Device Discovery**

You can add devices to DCR through Device Discovery.

Discovery Summary

Discovery status **Completed**
Discovery start time **Tue Dec 13 15:49:07 PST 2011**
Discovery end time **Tue Dec 13 15:59:33 PST 2011**
Total devices discovered **49**
Reachable devices **29**
Unreachable devices **20**
Devices newly added to DCR **29**
Devices updated in DCR **0**

Device Allocation Settings

Auto allocate all devices: Enabled

Device Addition

Devices in DCR: 29

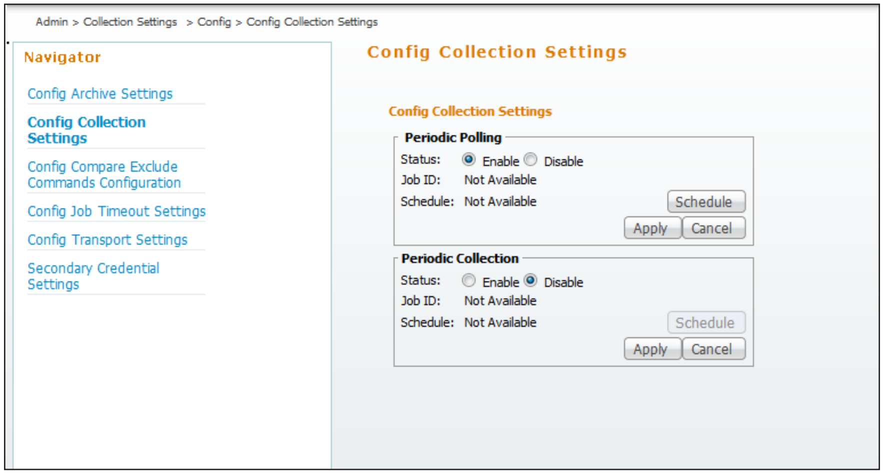
Devices on the network have been discovered and are ready for other management tasks such as asset, configuration, and software image management.

Procedure 7 Manage administrator tasks

Device configuration can occur on an as-needed or scheduled basis.

Step 1: Navigate to **Admin > Collection Settings > Config**.

Step 2: Click **Config Collection Settings**, and then under **Periodic Polling**, select the **Enable** check box.



Admin > Collection Settings > Config > Config Collection Settings

Config Collection Settings

Config Collection Settings

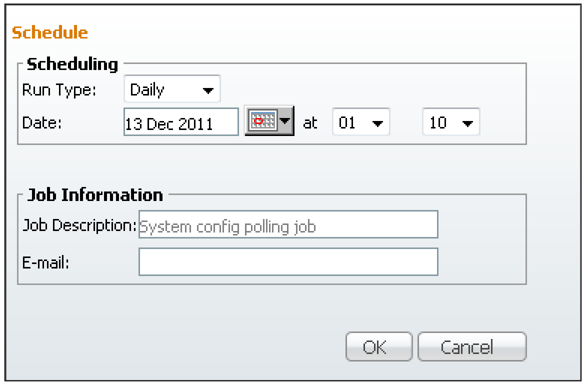
Periodic Polling
Status: ● Enable ○ Disable
Job ID: Not Available
Schedule: Not Available

Periodic Collection
Status: ○ Enable ● Disable
Job ID: Not Available
Schedule: Not Available

Navigator
Config Archive Settings
Config Collection Settings
Config Compare Exclude Commands Configuration
Config Job Timeout Settings
Config Transport Settings
Secondary Credential Settings
Schedule
Apply
Cancel
Schedule
Apply
Cancel

Step 3: Click **Schedule**.

Step 4: In the window that appears, set the time to a non-peak time on the network, and then click **OK**.



Schedule

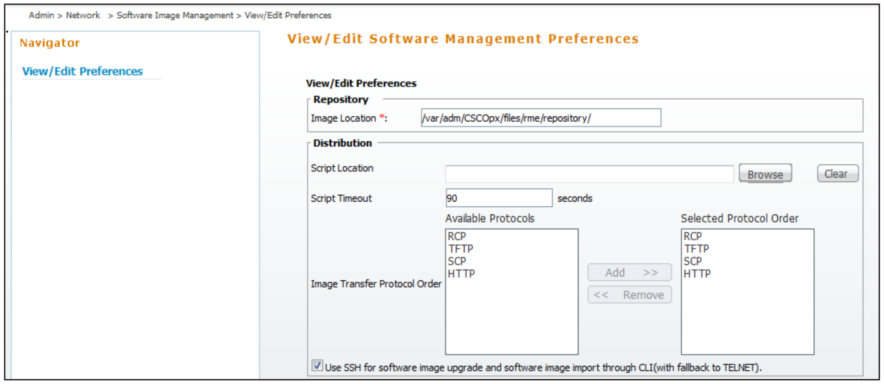
Scheduling
Run Type: Daily
Date: 13 Dec 2011 at 01 10

Job Information
Job Description: System config polling job
E-mail:

Step 5: Click **Apply**.

Step 6: Repeat Step 2 through Step 5 for **Periodic Collection**.

Step 7: Navigate to **Admin > Network > Software Image Management > View / Edit Preferences**, select the **Use SSH for software image upgrade and software image import through CLI(with fallback to TELNET**) check box, and then click **Apply**.



Admin > Network > Software Image Management > View/Edit Preferences

View/Edit Software Management Preferences

View/Edit Preferences

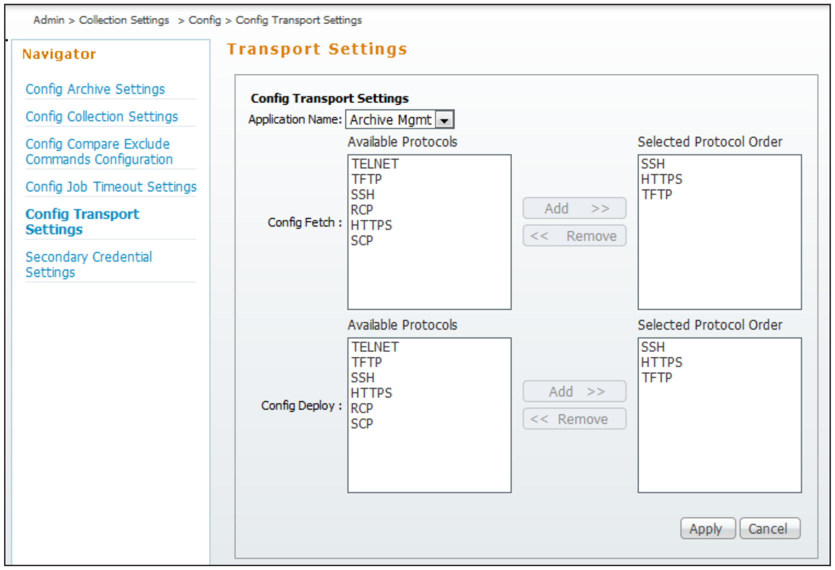
Repository
Image Location *: /var/adm/CSCOpx/files/rme/repository/

Distribution
Script Location
Script Timeout 90 seconds
Image Transfer Protocol Order
Available Protocols: RCP, TFTP, SCP, HTTP
Selected Protocol Order: RCP, TFTP, SCP, HTTP

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

Step 8: Navigate to **Admin > Collection Settings > Config > Config Transport Settings**.

Step 9: For each application in the **Application Name** list, adjust the selected protocol order to be **SSH, HTTPS, TFTP**, and then click **Apply**.



Admin > Collection Settings > Config > Config Transport Settings

Transport Settings

Config Transport Settings
Application Name: Archive Mgmt

Config Fetch :
Available Protocols: TELNET, TFTP, SSH, RCP, HTTPS, SCP
Selected Protocol Order: SSH, HTTPS, TFTP

Config Deploy :
Available Protocols: TELNET, TFTP, SSH, HTTPS, RCP, SCP
Selected Protocol Order: SSH, HTTPS, TFTP

Navigator
Config Archive Settings
Config Collection Settings
Config Compare Exclude Commands Configuration
Config Job Timeout Settings
Config Transport Settings
Secondary Credential Settings
Add >>
<< Remove
Add >>
<< Remove
Apply
Cancel

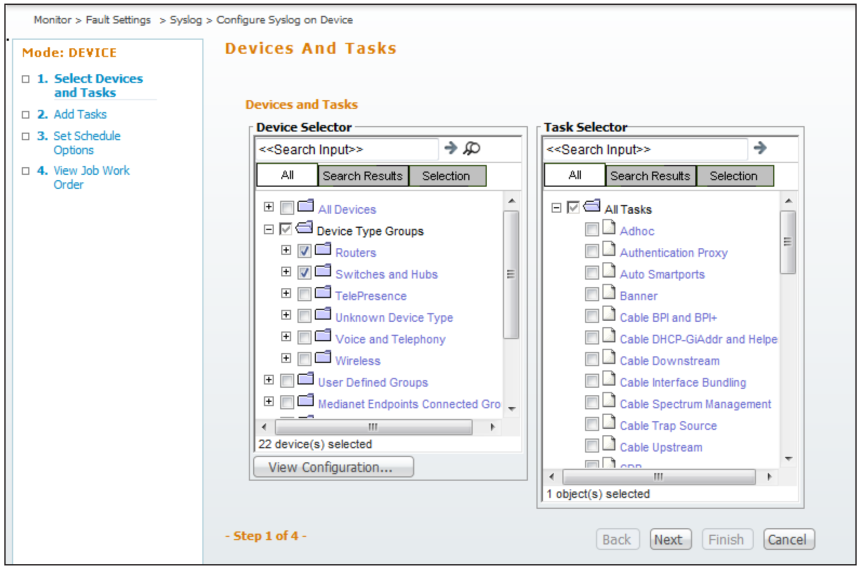
Procedure 8 Configure syslog collection

Step 1: Navigate to **Monitor > Fault Settings > Syslog > Configure Syslog on Device**.

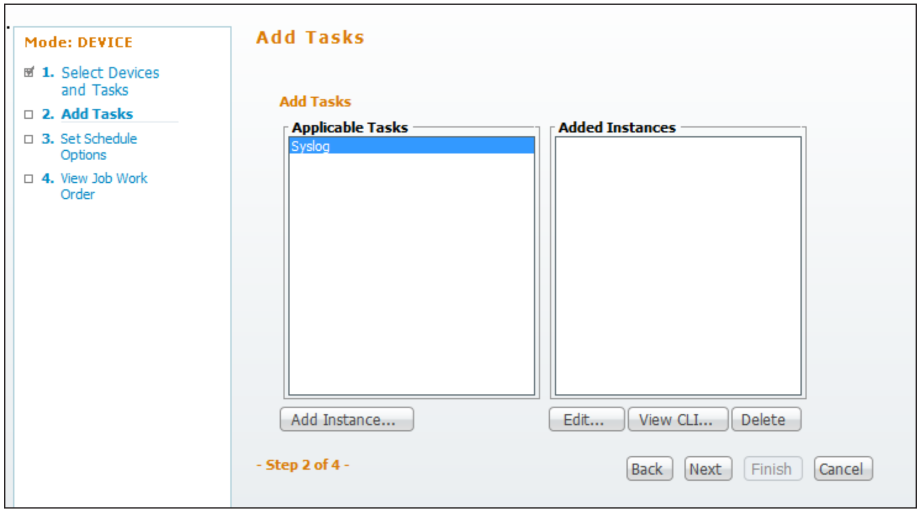
Step 2: Under **Device Selector**, expand **Device Type Groups**.

Step 3: Select **Router**.

Step 4: Select **Switches and Hubs**, and then click **Next**.



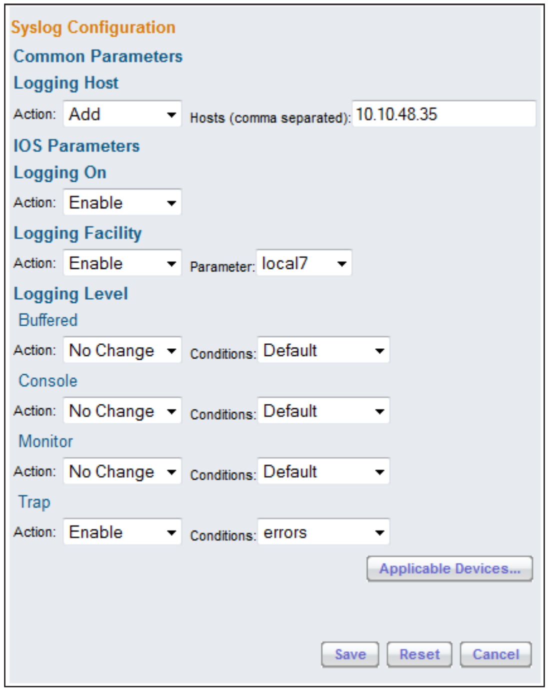
Step 5: Click **Add Instance**.



Step 6: In the Syslog Configuration window, configure these settings:

- Logging Host Action—**Add**
- Hosts— **10.10.48.35** (the Cisco LMS server)
- Logging On Action—**Enable**
- Logging Facility Action—**Enable**
- Parameter—**local7**
- Trap Action—**Enable**
- Conditions—**errors**

Step 7: Click **Save**.



Syslog Configuration

Common Parameters

Logging Host

Action: Add ▾ Hosts (comma separated): 10.10.48.35

IOS Parameters

Logging On

Action: Enable ▾

Logging Facility

Action: Enable ▾ Parameter: local7 ▾

Logging Level

Buffered

Action: No Change ▾ Conditions: Default ▾

Console

Action: No Change ▾ Conditions: Default ▾

Monitor

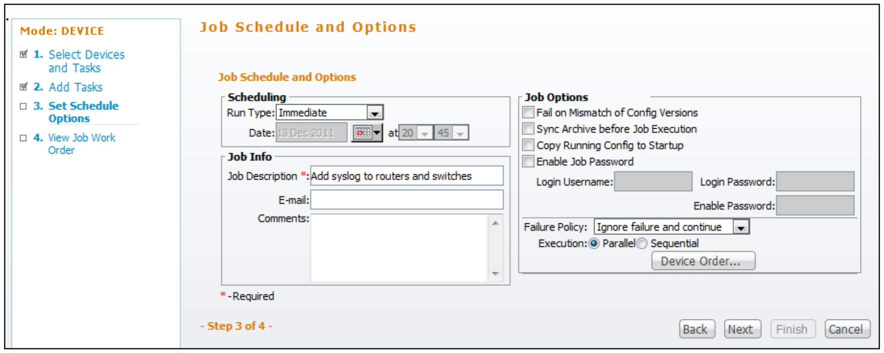
Action: No Change ▾ Conditions: Default ▾

Trap

Action: Enable ▾ Conditions: errors ▾

Step 8: Click **Next**.

Step 9: Enter a **Job Description** (for example, **Add syslog to routers and switches**), and then click **Next**.



Mode: DEVICE

- ☑ 1. Select Devices and Tasks
- ☑ 2. Add Tasks
- □ 3. Set Schedule Options
- □ 4. View Job Work Order

Job Schedule and Options

Job Schedule and Options

Scheduling

Run Type: Immediate ▾

Date: 13 Dec 2011 at 20 ▾ 45 ▾

Job Info

Job Description *: Add syslog to routers and switches

E-mail:

Comments:

* - Required

Job Options

- □ Fail on Mismatch of Config Versions
- □ Sync Archive before Job Execution
- □ Copy Running Config to Startup
- □ Enable Job Password

Login Username: Login Password:

Enable Password:

Failure Policy: Ignore failure and continue ▾

Execution: ● Parallel ○ Sequential

- Step 3 of 4 -

Step 10: Review the Job Work Order description, and then click **Finish**.

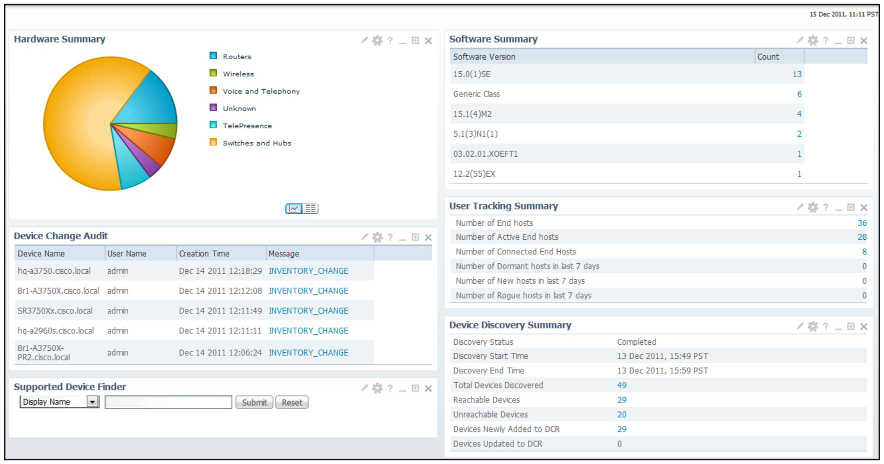
Step 11: To view the syslog messages, click **Monitor**.

Process

Managing the Network

1. Distribute software images
2. Customize monitoring
3. Generate and view reports
4. Deploy templates

Using the Inventory Dashboard, you can view all information regarding hardware, software, user tracking, device audit changes, device discovery, and support devices.



15 Dec 2011, 11:11 PST

Hardware Summary

Software Summary

Software Version	Count
15.0(1)SE	13
Generic Class	6
15.1(4)M2	4
5.1(3)N1(1)	2
03.02.01.XOEFT1	1
12.2(55)EX	1

User Tracking Summary

Number of End hosts	36
Number of Active End hosts	28
Number of Connected End Hosts	8
Number of Dormant hosts in last 7 days	0
Number of New hosts in last 7 days	0
Number of Rogue hosts in last 7 days	0

Device Change Audit

Device Name	User Name	Creation Time	Message
hq-a3750.cisco.local	admin	Dec 14 2011 12:18:29	INVENTORY_CHANGE
Br1-A3750X.cisco.local	admin	Dec 14 2011 12:12:08	INVENTORY_CHANGE
SR3750Xx.cisco.local	admin	Dec 14 2011 12:11:49	INVENTORY_CHANGE
hq-a2960s.cisco.local	admin	Dec 14 2011 12:11:11	INVENTORY_CHANGE
Br1-A3750X-PR2.cisco.local	admin	Dec 14 2011 12:06:24	INVENTORY_CHANGE

Device Discovery Summary

Discovery Status	Completed
Discovery Start Time	13 Dec 2011, 15:49 PST
Discovery End Time	13 Dec 2011, 15:59 PST
Total Devices Discovered	49
Reachable Devices	29
Unreachable Devices	20
Devices Newly Added to DCR	29
Devices Updated to DCR	0

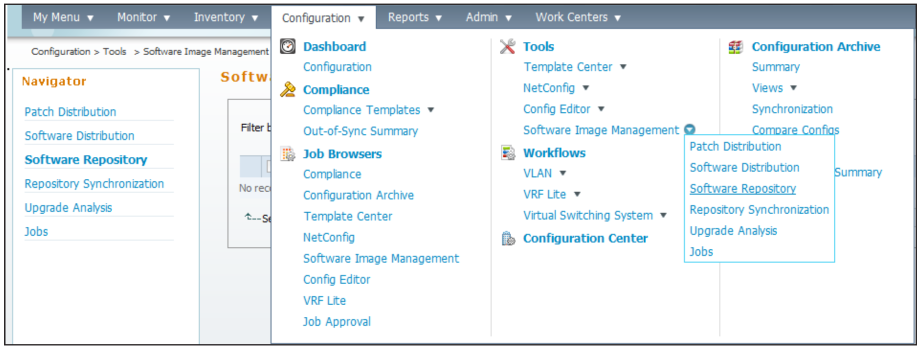
Supported Device Finder

Display Name ▾

Procedure 1 Distribute software images

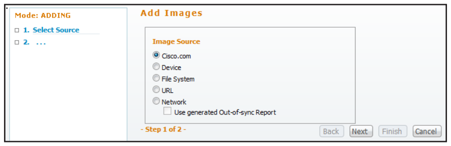
Software Image Management is a feature that enables you to push new images periodically to managed devices. This feature compares a managed device's existing image version with those in the Cisco LMS local software image repository or on cisco.com. Available upgrade options are shown, and Cisco LMS allows you to upgrade a managed device to an image through the GUI.

Step 1: To add an image to the local repository, navigate to **Configuration > Tools > Software Image Management > Software Repository**.



Step 2: To add software images to the repository (from cisco.com or a device, file system, or URL), click **Add**.

Step 3: Choose **Cisco.com** as the source from which you want to acquire the image, and then click **Next**.


Mode: ADDING

□ 1. Select Source
□ 2. ...

Add Images

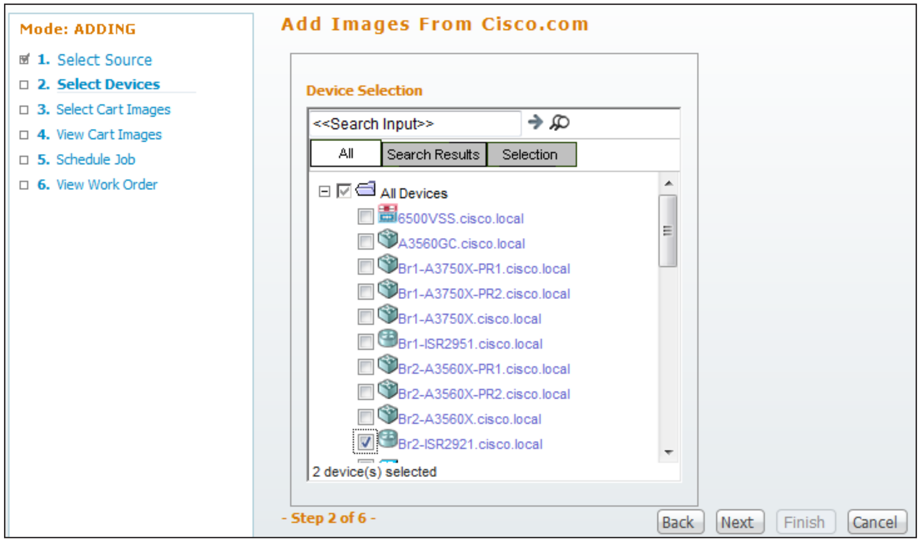
Image Source

● Cisco.com
○ Device
○ File System
○ URL
○ Network
□ Use generated Out-of-sync Report

- Step 1 of 2 -

Step 4: Enter a cisco.com username and password for an account that is entitled to download all software images that will be deployed to the network.

Step 5: In the Cisco LMS inventory, select a device, and then click **Next**.


Mode: ADDING

☑ 1. Select Source
□ 2. Select Devices
□ 3. Select Cart Images
□ 4. View Cart Images
□ 5. Schedule Job
□ 6. View Work Order

Add Images From Cisco.com

Device Selection

<<Search Input>>

☑ All Devices
- □ 6500VSS.cisco.local
- □ A3560GC.cisco.local
- □ Br1-A3750X-PR1.cisco.local
- □ Br1-A3750X-PR2.cisco.local
- □ Br1-A3750X.cisco.local
- □ Br1-ISR2951.cisco.local
- □ Br2-A3560X-PR1.cisco.local
- □ Br2-A3560X-PR2.cisco.local
- □ Br2-A3560X.cisco.local
- ☑ Br2-ISR2921.cisco.local

2 device(s) selected

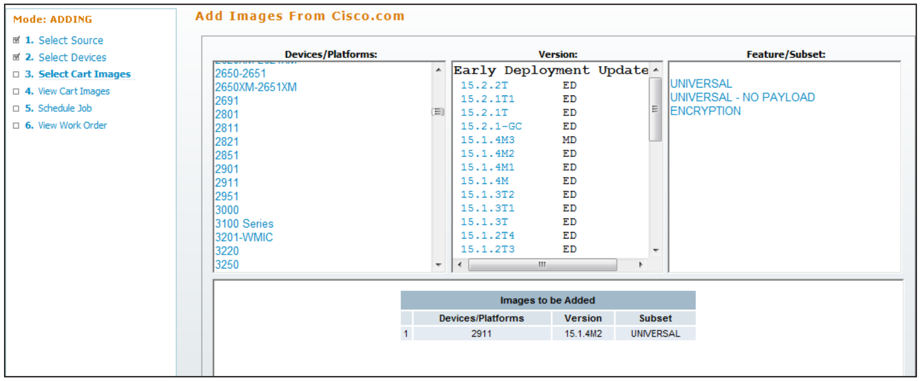
- Step 2 of 6 -

Step 6: In the **Device/Platforms** pane, select the device name.

Step 7: In the **Version** pane, select the software version.

Step 8: In the **Feature/Subset** pane, select the software feature set.

Step 9: Click **Next**.


Mode: ADDING

☑ 1. Select Source
☑ 2. Select Devices
□ 3. Select Cart Images
□ 4. View Cart Images
□ 5. Schedule Job
□ 6. View Work Order

Add Images From Cisco.com

Devices/Platforms:

2650-2651
2650XM-2651XM
2691
2801
2811
2821
2851
2901
2911
2951
3000
3100 Series
3201-WMIC
3220
3250

Version:

```
Early Deployment Update
  15.2.2T        ED
  15.2.1T1       ED
  15.2.1T        ED
  15.2.1-GC      ED
  15.1.4M3       MD
  15.1.4M2       ED
  15.1.4M1       ED
  15.1.4M        ED
  15.1.3T2       ED
  15.1.3T1       ED
  15.1.3T        ED
  15.1.2T4       ED
  15.1.2T3       ED
```

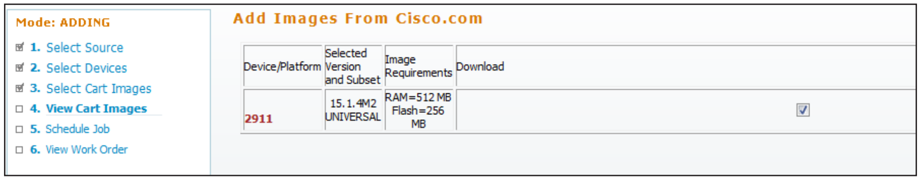
Feature/Subset:

UNIVERSAL
UNIVERSAL - NO PAYLOAD ENCRYPTION

Images to be Added

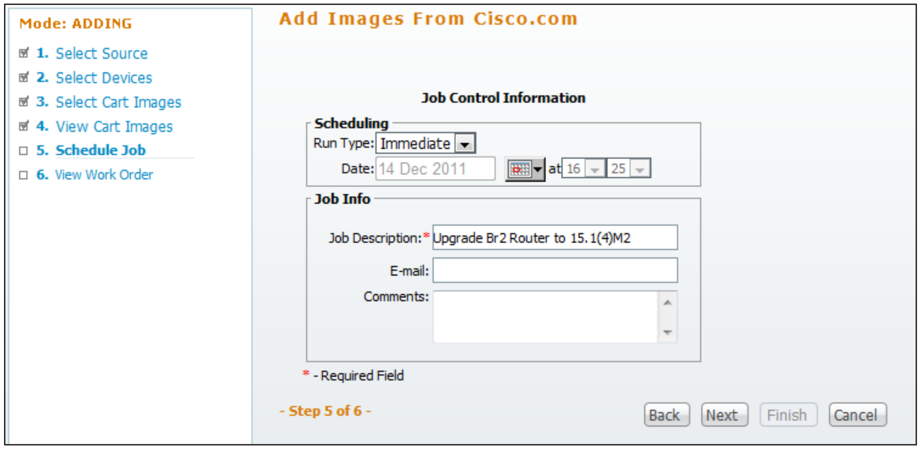
	Devices/Platforms	Version	Subset
1	2911	15.1.4M2	UNIVERSAL

Step 10: Ensure that the check box in the **Download** column is selected, and then click **Next**.



Device/Platform	Selected Version and Subset	Image Requirements	Download
2911	15.1.4M2 UNIVERSAL	RAM=512 MB Flash=256 MB	☑

Step 11: Enter a Job Description, and then click **Next**.



Job Control Information

Scheduling

Run Type: Immediate

Date: 14 Dec 2011 at 16 25

Job Info

Job Description:* Upgrade Br2 Router to 15.1(4)M2

E-mail:

Comments:

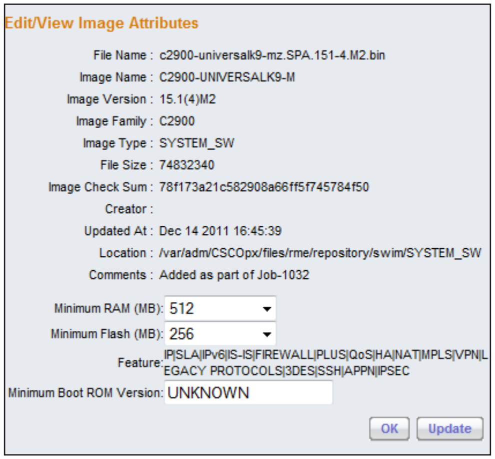
* - Required Field

- Step 5 of 6 -

Step 12: Review the Work Order, and then click **Finish**.

Step 13: Return to **Software Repository Management** and click the name of the software image that was added in Step 8. Make sure that the device requirements are set correctly.

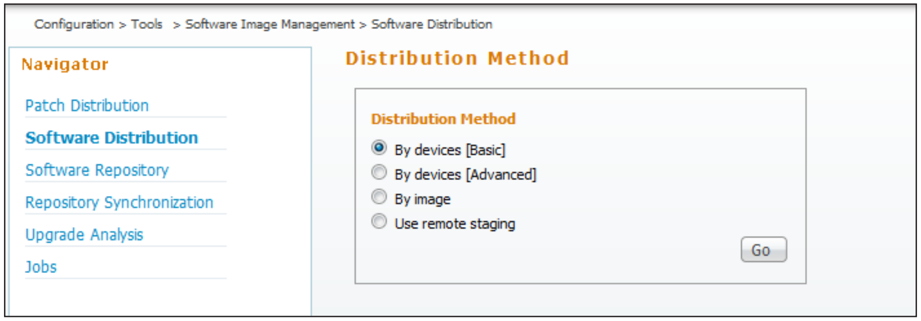
Step 14: Set the Minimum Ram and Minimum Flash values to the correct values if they are incorrect, and then click **Update**.



File Name : c2900-universalk9-mz.SPA.151-4.M2.bin
Image Name : C2900-UNIVERSALK9-M
Image Version : 15.1(4)M2
Image Family : C2900
Image Type : SYSTEM_SW
File Size : 74832340
Image Check Sum : 78f173a21c582908a66ff5f745784f50
Creator :
Updated At : Dec 14 2011 16:45:39
Location : /var/adm/CSCOpx/files/rme/repository/swim/SYSTEM_SW
Comments : Added as part of Job-1032
Minimum RAM (MB): 512
Minimum Flash (MB): 256
Feature: IP|SLA|IPv6|IS-IS|FIREWALL|PLUS|QoS|HA|NAT|MPLS|VPN|LEGACY PROTOCOLS|3DES|SSH|APPN|IPSEC
Minimum Boot ROM Version: UNKNOWN

Step 15: Navigate to **Configuration > Tools > Software Image Management > Software Distribution**.

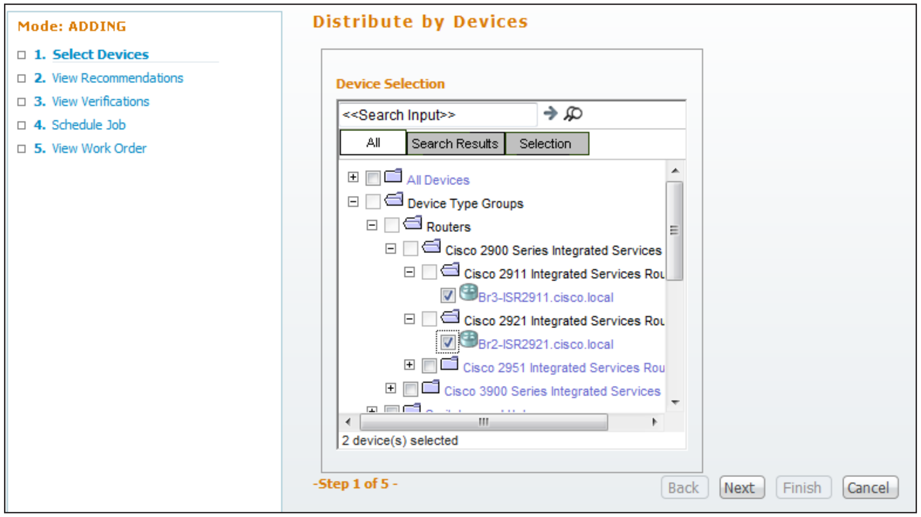
Step 16: Click **Software Distribution**, select **By Devices [Basic]**, and then click **Go**.



Distribution Method

● By devices [Basic]
○ By devices [Advanced]
○ By image
○ Use remote staging

Step 17: Choose the device or devices for image distribution, and then click **Next**.



Mode: ADDING

- □ 1. Select Devices
- □ 2. View Recommendations
- □ 3. View Verifications
- □ 4. Schedule Job
- □ 5. View Work Order

Distribute by Devices

Device Selection

<<Search Input>>

All | Search Results | Selection

- ⊞ □ All Devices
- ⊟ □ Device Type Groups
  - ⊟ □ Routers
    - ⊟ □ Cisco 2900 Series Integrated Services
      - ⊟ □ Cisco 2911 Integrated Services Rou
        - ☑ Br3-ISR2911.cisco.local
      - ⊟ □ Cisco 2921 Integrated Services Rou
        - ☑ Br2-ISR2921.cisco.local
      - ⊞ □ Cisco 2951 Integrated Services Rou
    - ⊞ □ Cisco 3900 Series Integrated Services

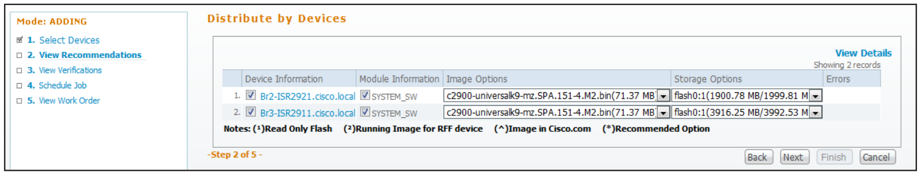
2 device(s) selected

-Step 1 of 5 -

Step 18: On the page that appears, enter your cisco.com credentials, and then click **OK**.

Cisco LMS shows the images available in the software repository for the selected device or devices.

Step 19: Select the image to which you would like to upgrade the device, and then click **Next**.



Mode: ADDING

- ☑ 1. Select Devices
- □ 2. View Recommendations
- □ 3. View Verifications
- □ 4. Schedule Job
- □ 5. View Work Order

Distribute by Devices

View Details

Showing 2 records

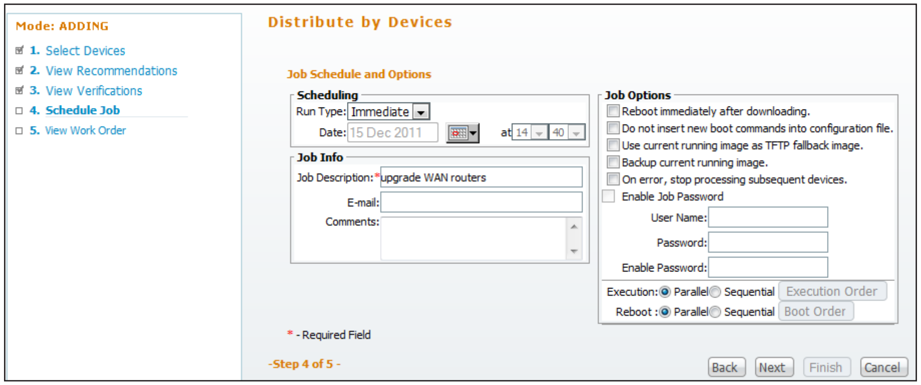
	Device Information	Module Information	Image Options	Storage Options	Errors
1.	☑ Br2-ISR2921.cisco.local	☑ SYSTEM_SW	c2900-universalk9-mz.SPA.151-4.M2.bin(71.37 MB	flash0:1(1900.78 MB/1999.81 M	
2.	☑ Br3-ISR2911.cisco.local	☑ SYSTEM_SW	c2900-universalk9-mz.SPA.151-4.M2.bin(71.37 MB	flash0:1(3916.25 MB/3992.53 M	

Notes: (¹)Read Only Flash (²)Running Image for RFF device (^)Image in Cisco.com (*)Recommended Option

-Step 2 of 5 -

Step 20: In the Notifications window, click any failures or warnings for the software distribution, and then click **Next**.

Step 21: If you want select options based on your organization's scheduling policy, you can do so on the Job Schedule and Options page, and then click **Next.**



Mode: ADDING

- ☑ 1. Select Devices
- ☑ 2. View Recommendations
- ☑ 3. View Verifications
- □ 4. Schedule Job
- □ 5. View Work Order

Distribute by Devices

Job Schedule and Options

Scheduling

Run Type: Immediate

Date: 15 Dec 2011 at 14 40

Job Info

Job Description:* upgrade WAN routers

E-mail:

Comments:

Job Options

- □ Reboot immediately after downloading.
- □ Do not insert new boot commands into configuration file.
- □ Use current running image as TFTP fallback image.
- □ Backup current running image.
- □ On error, stop processing subsequent devices.
- □ Enable Job Password

User Name:

Password:

Enable Password:

Execution: ● Parallel ○ Sequential Execution Order

Reboot : ● Parallel ○ Sequential Boot Order

* - Required Field

-Step 4 of 5 -

Step 22: A new page shows the work order that was just created. To complete the work order, click **Finish**.

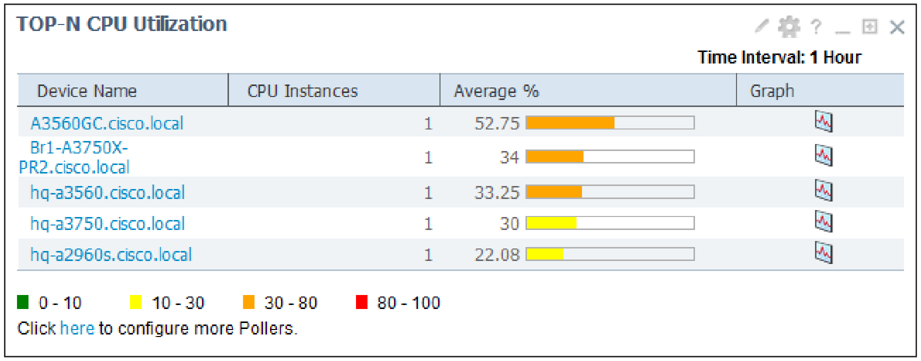
Procedure 2 Customize monitoring

Monitoring plays a big role in any network management process, and the Monitoring Dashboard provides a unified view of all the activities being monitored by an administrator. Cisco LMS has a comprehensive list of monitoring portlets from a device level to the network level—such as device and interface availability; high severity alerts; memory, CPU and interface use; performance threshold; fault summary; IPSLA violation reports; and syslog information.

You can customize these activities based on your network needs. This procedure describes one such activity, CPU utilization.

Step 1: To access the Monitoring Dashboard, navigate to **Monitor > Dashboards >Monitoring**.

Step 2: By default, you can view a list of devices with the top CPU utilization on the dashboard.



TOP-N CPU Utilization

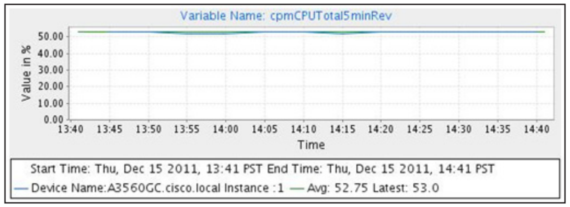
Time Interval: 1 Hour

Device Name	CPU Instances	Average %	Graph
A3560GC.cisco.local	1	52.75	📈
Br1-A3750X-PR2.cisco.local	1	34	📈
hq-a3560.cisco.local	1	33.25	📈
hq-a3750.cisco.local	1	30	📈
hq-a2960s.cisco.local	1	22.08	📈

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

Click here to configure more Pollers.

Step 3: For the details of the CPU utilization for a specific device, click the **Graph** icon.



Start Time: Thu, Dec 15 2011, 13:41 PST End Time: Thu, Dec 15 2011, 14:41 PST

— Device Name:A3560GC.cisco.local Instance :1 — Avg: 52.75 Latest: 53.0

Procedure 3 Generate and view reports

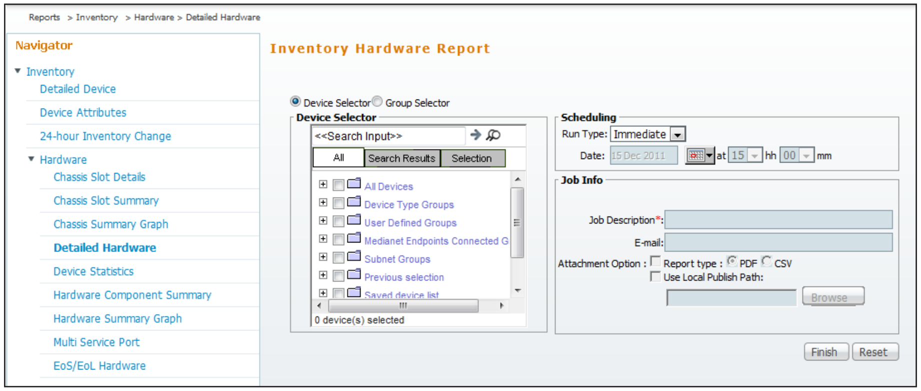
Cisco LMS provides you a single launch point for all reports that you can generate and view. The Reports menu provides the following options:

- Inventory Report—Contains reports pertaining to devices, hardware, and end-of-sale and end-of-life information
- Switch Port—Contains reports on switch capacity, switch port summary, and utilization history
- Technology—Contains reports for technologies like EnergyWise, Identity, Power over Ethernet, and VRF Lite
- Fault and Event—Contains information about threshold violation, device fault, syslog., and PSIRT
- Performance—Contains information about CPU and interface utilization, interface error, and IPSLA
- System—Contains information about the number of users logged in, collection detail, configuration file changes, and 24-hour change
- Audit—Contains audit reports for software image distribution and download history
- Report Designer—Generates custom reports, especially for syslog and inventory
- Cisco—Allows you to check contract information and bug status using the bug toolkit
- View Report Archives—Is a report that is created from a scheduled report and stored in report archive

In this example, you generate an inventory report:

Step 1: Navigate to **Reports > Inventory > Hardware > Detailed Hardware**.

Step 2: Select **All Devices**, and then click **Finish**.



Inventory Hardware Report

● Device Selector ○ Group Selector

Device Selector

<<Search Input>>

0 device(s) selected

Scheduling

Run Type: Immediate

Date: 15 Dec 2011 at 15 hh 00 mm

Job Info

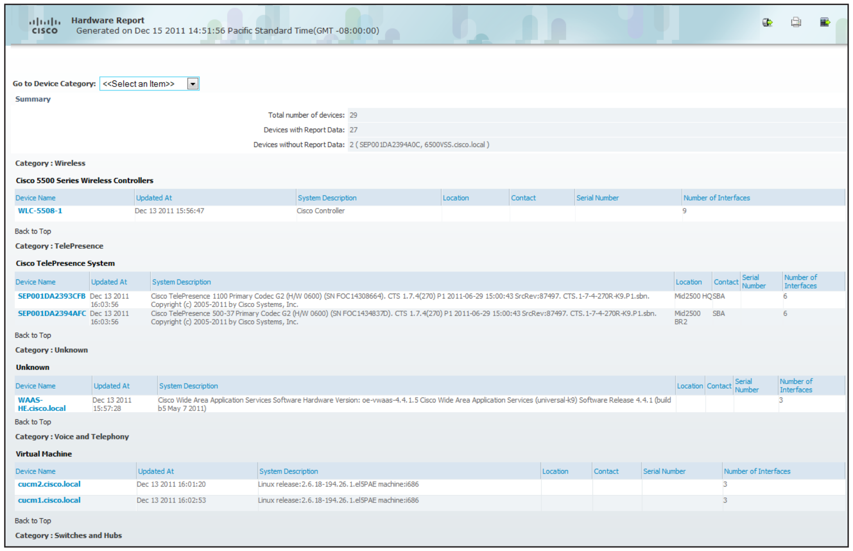
Job Description*:

E-mail:

Attachment Option : □ Report type : ● PDF ○ CSV

□ Use Local Publish Path:

Cisco LMS generates a detailed hardware report, providing information about the device—system description, RAM, image running, etc.



Hardware Report
Generated on Dec 15 2011 14:51:56 Pacific Standard Time(GMT -08:00:00)

Go to Device Category: <<Select an Item>>

Summary

Total number of devices:	29
Devices with Report Data:	27
Devices without Report Data:	2 (SEP001DA2394A0C, 6500VSS.cisco.local)

Category : Wireless

Cisco 5500 Series Wireless Controllers

Device Name	Updated At	System Description	Location	Contact	Serial Number	Number of Interfaces
WLC-5508-1	Dec 13 2011 15:56:47	Cisco Controller				9

Back to Top

Category : TelePresence

Cisco TelePresence System

Device Name	Updated At	System Description	Location	Contact	Serial Number	Number of Interfaces
SEP001DA2393CFB	Dec 13 2011 16:03:56	Cisco TelePresence 1100 Primary Codec G2 (H/W 0600) (SN FOC14308664). CTS 1.7.4(270) P1 2011-06-29 15:00:43 SrcRev:87497. CTS.1-7-4-270R-K9.P1.sbn. Copyright (c) 2005-2011 by Cisco Systems, Inc.	Mid2500 HQ	SBA		6
SEP001DA2394AFC	Dec 13 2011 16:03:56	Cisco TelePresence 500-37 Primary Codec G2 (H/W 0600) (SN FOC1434837D). CTS 1.7.4(270) P1 2011-06-29 15:00:43 SrcRev:87497. CTS.1-7-4-270R-K9.P1.sbn. Copyright (c) 2005-2011 by Cisco Systems, Inc.	Mid2500 BR2	SBA		6

Back to Top

Category : Unknown

Unknown

Device Name	Updated At	System Description	Location	Contact	Serial Number	Number of Interfaces
WAAS-HE.cisco.local	Dec 13 2011 15:57:28	Cisco Wide Area Application Services Software Hardware Version: oe-vwaas-4.4.1.5 Cisco Wide Area Application Services (universal-k9) Software Release 4.4.1 (build b5 May 7 2011)				3

Back to Top

Category : Voice and Telephony

Virtual Machine

Device Name	Updated At	System Description	Location	Contact	Serial Number	Number of Interfaces
cucm2.cisco.local	Dec 13 2011 16:01:20	Linux release:2.6.18-194.26.1.el5PAE machine:i686				3
cucm1.cisco.local	Dec 13 2011 16:02:53	Linux release:2.6.18-194.26.1.el5PAE machine:i686				3

Back to Top

Category : Switches and Hubs

Procedure 4 Deploy templates

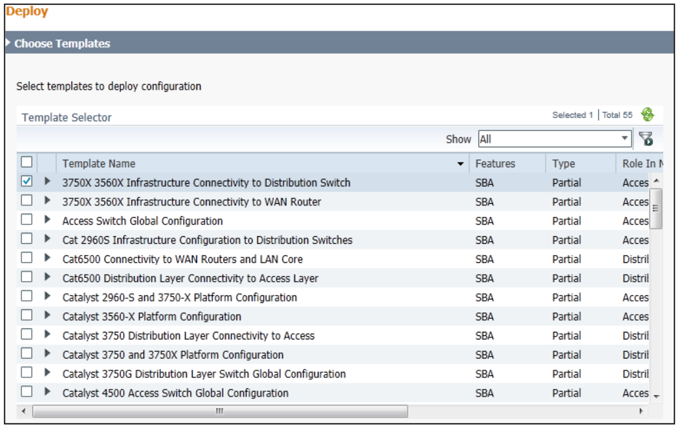
Another important feature, Templates, is specifically designed for deploying configurations in networks that consist of large numbers of similar devices. It is an enormous task for administrators to configure each of these devices individually. Ideally, administrators would like to have a set of templates with standard (or global) configurations that are common to certain devices in the network. Using these templates, administrators can quickly deploy the configuration, thus saving a lot of time as well as avoiding configuration errors that may happen during manual configuration.

Cisco LMS provides system-defined or user-defined templates, which are in the form of .xml files. You can customize these templates to accommodate your needs. This procedure focuses on importing and deploying templates that are specific to Cisco SBA.

Templates based on the *Cisco SBA for Midsize Organizations— Borderless Networks Foundation Deployment Guide* are included as part of Cisco LMS. You can also edit the templates or even create an entirely new template. If you choose to create a customized template, you do it manually by creating it in an .xml file.

Step 1: In the Cisco LMS portal, navigate to **Configuration > Tools > Template Center**.

Step 2: Click **Deploy**, choose the template that you would like to deploy, and then click **Next**.



Deploy

Choose Templates

Select templates to deploy configuration

Template Selector — Selected 1 | Total 55

Show: All

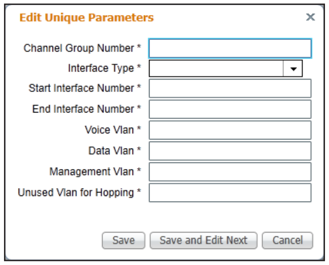
☐		Template Name	Features	Type	Role In N
☑	▶	3750X 3560X Infrastructure Connectivity to Distribution Switch	SBA	Partial	Acces
☐	▶	3750X 3560X Infrastructure Connectivity to WAN Router	SBA	Partial	Acces
☐	▶	Access Switch Global Configuration	SBA	Partial	Acces
☐	▶	Cat 2960S Infrastructure Configuration to Distribution Switches	SBA	Partial	Acces
☐	▶	Cat6500 Connectivity to WAN Routers and LAN Core	SBA	Partial	Distril
☐	▶	Cat6500 Distribution Layer Connectivity to Access Layer	SBA	Partial	Distril
☐	▶	Catalyst 2960-S and 3750-X Platform Configuration	SBA	Partial	Acces
☐	▶	Catalyst 3560-X Platform Configuration	SBA	Partial	Acces
☐	▶	Catalyst 3750 Distribution Layer Connectivity to Access	SBA	Partial	Distril
☐	▶	Catalyst 3750 and 3750X Platform Configuration	SBA	Partial	Distril
☐	▶	Catalyst 3750G Distribution Layer Switch Global Configuration	SBA	Partial	Distril
☐	▶	Catalyst 4500 Access Switch Global Configuration	SBA	Partial	Acces

Tech Tip

Some of the templates are intended for devices that are specific to the *Cisco SBA for Enterprise Organizations— Borderless Networks LAN Deployment Guide*. Be certain that you are applying a template that is relevant to the *Cisco SBA for Midsize Organizations— Borderless Networks Foundation Deployment Guide*.

Step 3: In Device Selector, choose the devices to which you want to push these templates, and then click **Next**.

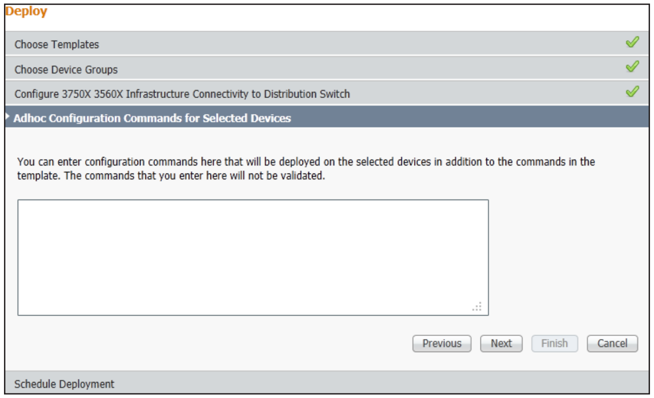
Step 4: A page appears that requires you to provide the variables for the commands for that particular template. In this example, LAN Switch Global Template has the variables shown. Fill in the required variables, and then click **Save and Edit Next**.



Edit Unique Parameters

Channel Group Number *	
Interface Type *	
Start Interface Number *	
End Interface Number *	
Voice Vlan *	
Data Vlan *	
Management Vlan *	
Unused Vlan for Hopping *	

Step 5: The Deploy page lets you enter configuration commands that will be deployed on the selected devices in addition to the commands in the template.



Deploy

Choose Templates ✓

Choose Device Groups ✓

Configure 3750X 3560X Infrastructure Connectivity to Distribution Switch ✓

Adhoc Configuration Commands for Selected Devices

You can enter configuration commands here that will be deployed on the selected devices in addition to the commands in the template. The commands that you enter here will not be validated.

Step 6: To deploy the template on the selected device, click **Finish**. The template will be deployed based on the scheduled settings. If you choose the email option, Cisco LMS will send a confirmation email to the specified administrator.

Appendix A: Prime LMS Deployment Guide Product List

Functional Area	Product	Part Numbers	Software Version
Network Management	Cisco LAN Management Solution	R-LMS-4.1-100-K9 Cisco Prime LMS 4.1 Base download - 100 device license	4.1
Network Management	Cisco LAN Management Solution	R-LMS-4.1-500-K9 Cisco Prime LMS 4.1 Base download - 500 device license	4.1
Network Management	Cisco LAN Management Solution	R-LMS-4.1-1K-K9 Cisco Prime LMS 4.1 Base download - 1000 device license	4.1

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**