Prime Infrastructure

TECHNOLOGY DESIGN GUIDE

August 2013

VALIDATED DESIGN

Table of Contents

Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. 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 at a CLI or script prompt appear as follows:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

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 feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Managing LAN and WAN Devices**—Cisco Prime LAN Management Solution (LMS) provides IT staff with a tool to manage LAN and WAN devices.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Managing device configuration and monitoring
- Managing syslog configuration and collection
- Managing software images

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Routing and Switching**—1 to 3 years installing, configuring, and maintaining routed and switched networks

Related CVD Guides

Campus Wired LAN Technology Design Guide

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd

Introduction

Technology Use Case

Organizations find it more challenging than ever to enable efficiency and productivity for information technology staff due to data network management complexity. Today's network can have multiple services running on the infrastructure, and as the network and number of services continue to evolve, data network management becomes even more critical for operational efficiency. IT staff must be able to adapt to an evolving network while ensuring existing operations are monitored, and have the flexibility to quickly isolate and fix network performance issues. These management needs fall into different use cases, such as network configuration, deployment, asset management, and troubleshooting. 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.

Use Case: Managing LAN and WAN Devices

Cisco Prime LMS provides the IT staff with a tool to manage their LAN and WAN devices and supports up to 10,000 devices.

This design guide enables the following network capabilities:

- **Manage device configuration**—Create backups for device configurations, and then retrieve the configurations so they can be reused or modified for deploying new devices.
- **Manage syslog configuration and collection**—Enable syslog messages on devices and forward messages to Cisco Prime LMS in order to improve troubleshooting when issues arise.
- **Manage software images**-–Push new images to devices by using the software image management feature.
- **Customize monitoring**-–Control the type of information displayed on the monitoring dashboard in Cisco Prime LMS, such as CPU and interface utilization, device availability, and faults.
- **Generate and view reports**—Use the default reports that can be generated in Cisco Prime LMS, such as inventory, fault and event, performance, and compliance.
- **Manage configuration templates**—Customize standard configuration templates provided with Cisco Prime LMS in order to configure desired features on the device. This feature allows the user to change the configuration on multiple devices simultaneously.

Design Overview

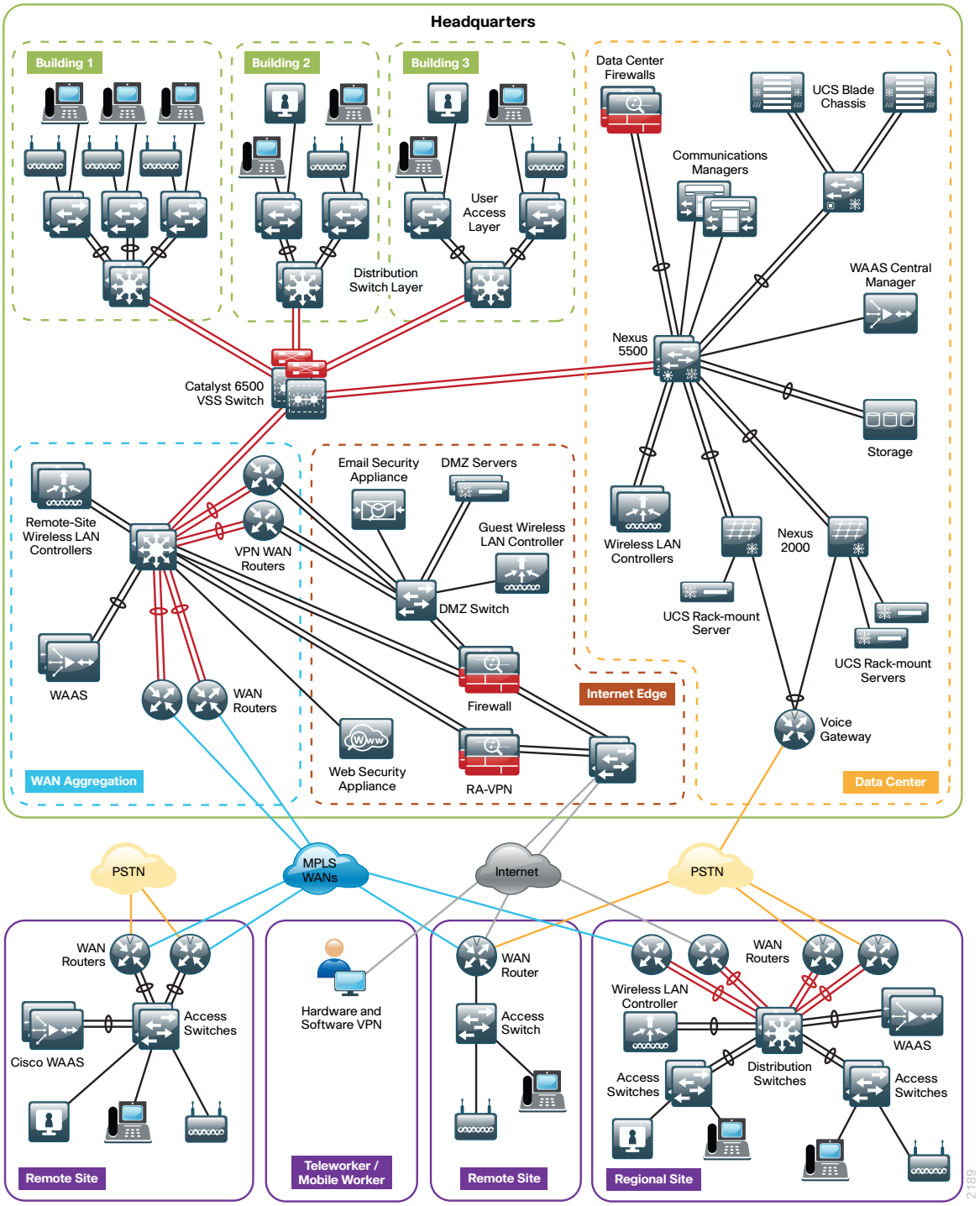
Cisco Prime LAN Management Solution (Prime LMS) is an integrated approach to network management tools for configuration, deployment, asset management, and troubleshooting. Prime LMS provides an intuitive GUI that can be accessed from anywhere from within the network and gives you a full view of a network use and performance.

This guide adds to the example configuration already built in the core Cisco Validated Design (CVD) guides. This supplemental guide includes:

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

Figure 1 depicts the CVD architecture overview. With such a network and services on top of it, network management applications like Prime LMS play a critical role in day-to-day network operations. Prime 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, Prime LMS allows network administrators to manage Cisco networks for customers through a browser-based interface that be accessed from anywhere at any time within the network.

Figure 1 - CVD Architecture Overview



The following sections describe the tasks this guide covers.

Installation and Deployment

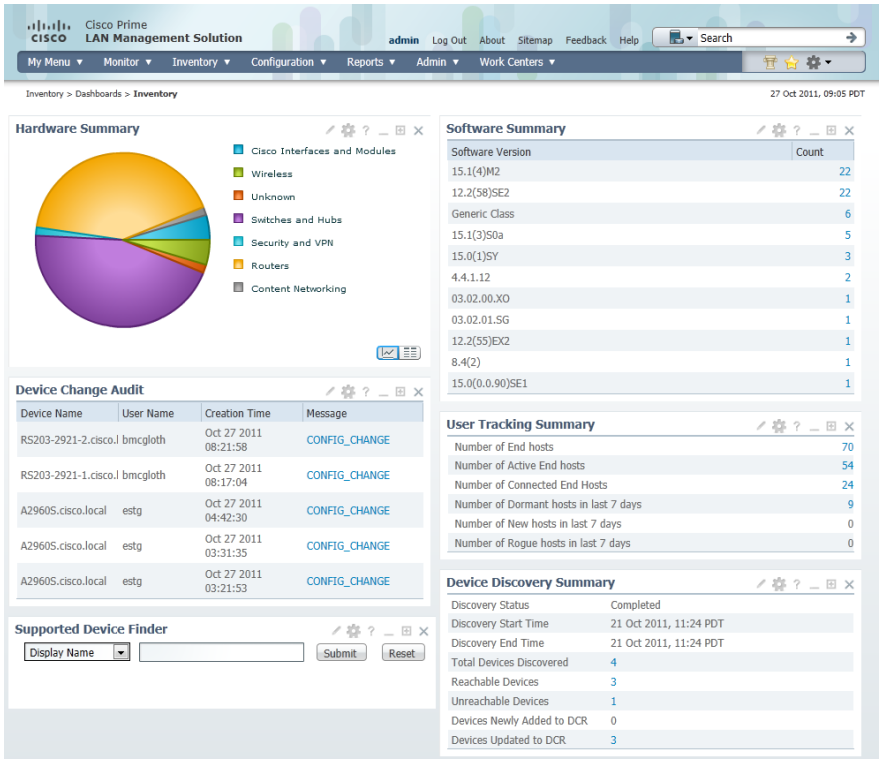
Most often, network administrators are unsure of the most efficient method to configure Prime LMS. Prime LMS provides a very important feature: the Getting Started workflow. This guided sequence eliminates configuration guesswork and assists you in performing essential and optional configuration and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

Configuration and Inventory Management

As networks grow, network administrators have a tedious job in keeping track of devices being added to or removed from the network. Administrators have to ensure that the devices are running proper software and that configurations are archived, and they must also implement network compliance by enforcing policies across the network. Prime LMS plays an important role in the end-to-end management of business-critical technologies and services. It aligns management functionality with the way that IT staff does their jobs. The following primary functions are included in the workflow and enable IT staff to achieve greater efficiency:

- 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 Prime 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.

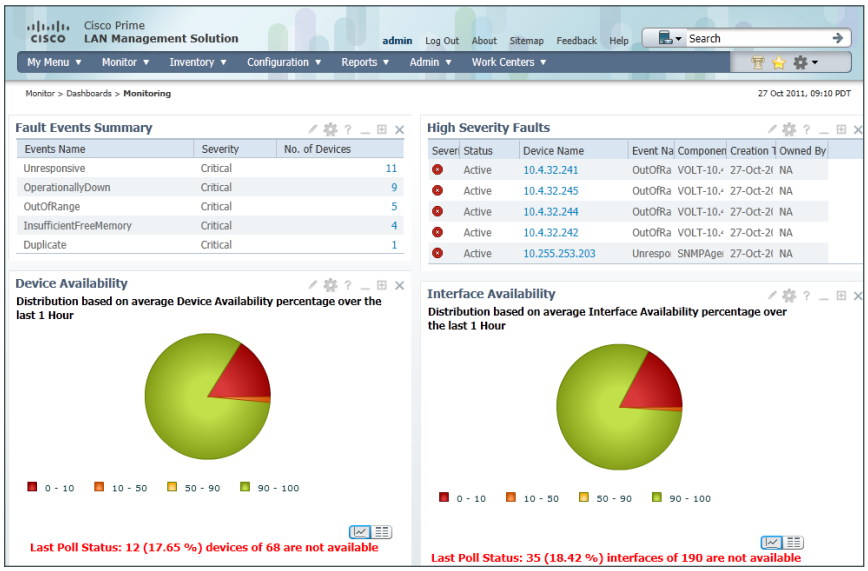
Figure 2 - Inventory Dashboard



Monitoring and Fault Management

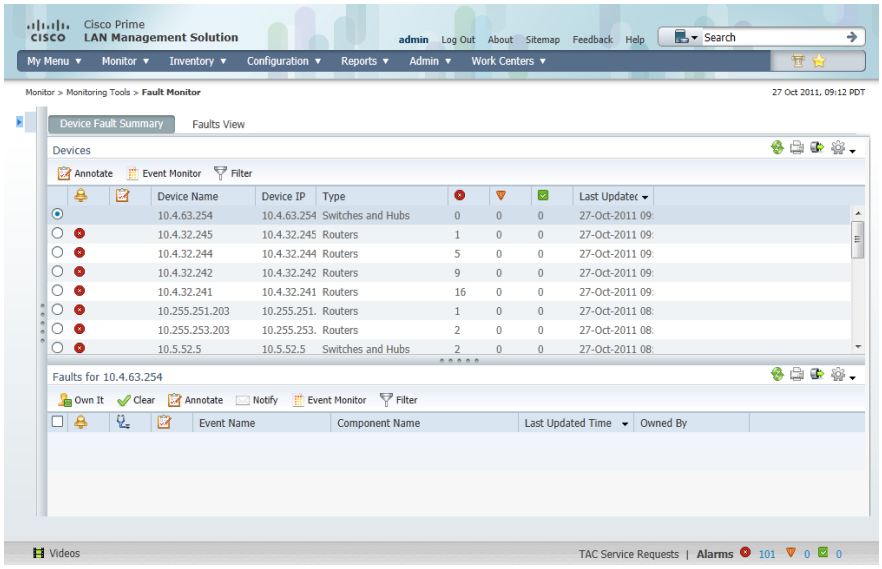
A network administrator's most important tasks are to ensure high network availability and to isolate and resolve any network issues before they affect services. Prime LMS provides both monitoring and fault management functionalities, using Simple Network Management Protocol (SNMP) polling and traps. The Prime 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



Prime 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



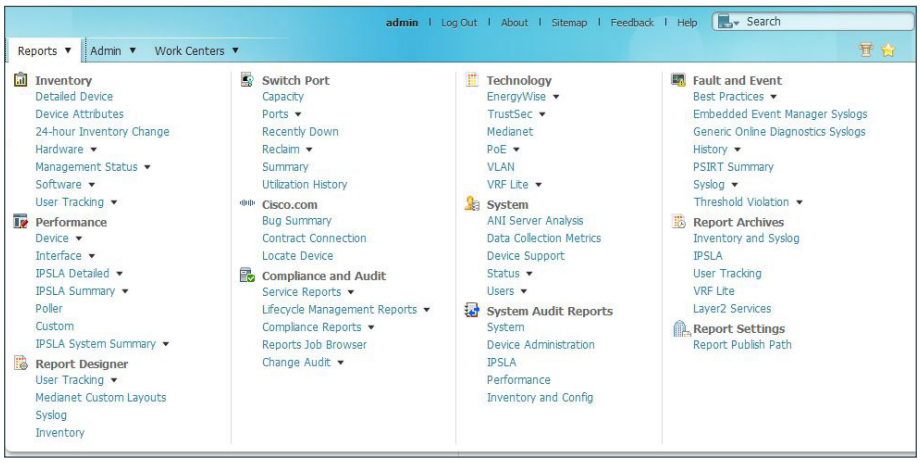
Templates

Administrators often 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. Prime 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 Prime LMS.

Reporting

Prime 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.

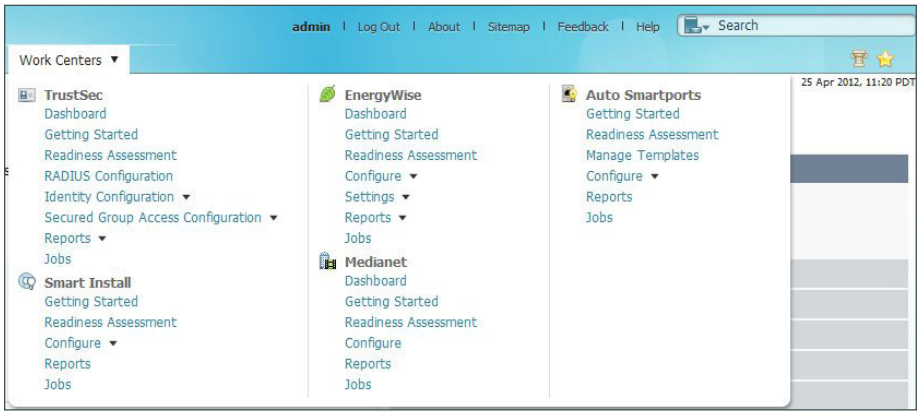
Figure 5 - Report Generation and View Layout



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



Deployment Details

PROCESS

Installing and Configuring Cisco Prime LMS

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

Procedure 1 Obtain a license

Cisco Prime LMS offers a single software installation that can manage up to 10,000 devices. Software licensing allows you to evaluate the software before deciding how you want to proceed: purchasing the license, piloting a small deployment before rolling it 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 Prime LMS evaluation software and ordering a digital PAK**—Download an evaluation copy of Prime 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 Prime LMS soft appliance by using the LMS Open Virtualization Archive (OVA) image from the LMS DVD. Before installing, please note that the following:

- Make sure that your system meets the recommended hardware and software specifications listed in the Prime LMS release notes.
- It takes 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.

Tech Tip

You need not install any soft appliance image on the virtual machine (VM) before installing Prime LMS, because the LMS OVA image has an embedded RedHat Enterprise soft appliance.

It is recommended you do the following before installing the Prime LMS soft appliance:

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

Step 1: Install and power on the Prime LMS OVA on the VMware ESX/ESXi server using VMware 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 (Example: LMS)
- IP Address (Example: 10.4.48.35)
- IP Netmask (Example: 255.255.255.0)
- Default Gateway (Example: 10.4.48.1)
- DNS Domain Name (Example: cisco.local)
- Primary Name Server (Example: 10.4.48.10)
- Add/Edit another name server? Y/N (Example: N)
- Primary NTP Server (Example: 10.4.48.17)
- System Time Zone (Example: America/Los_Angeles)

Step 4: Enter the username to access the Prime 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 is set as the shell password.

Step 6: Enter and confirm the password for the admin account to use to log in to Prime LMS using the browser. This password must contain a minimum of five characters and is also 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 takes 15 to 20 minutes to process the database engine, and then the server automatically reboots.

Procedure 3 Configure basic settings

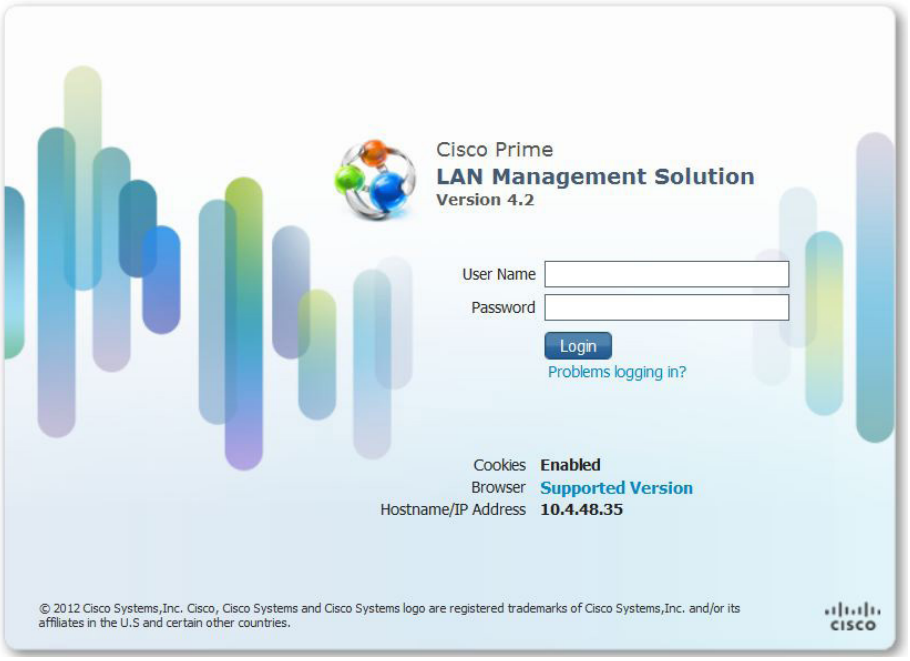
Step 1: On the client machine's web browser, disable any pop-up blockers and ensure that JavaScript is enabled.

To enable JavaScript:

- In Internet Explorer 8 or later, navigate to **Tools > Internet Options > Security > Custom level > Settings**, and then under **Scripting of Java applets**, select **Enable**.
- In Mozilla Firefox 9.x, navigate to **Tools > Option > Content**, and then select **Enable JavaScript**.

Step 2: Open the Prime LMS portal in your web browser. The browser reaches the Prime LMS portal by appending the port number 1741 to the DNS host name of the server on which you installed Prime LMS. Example: lms.cisco.local

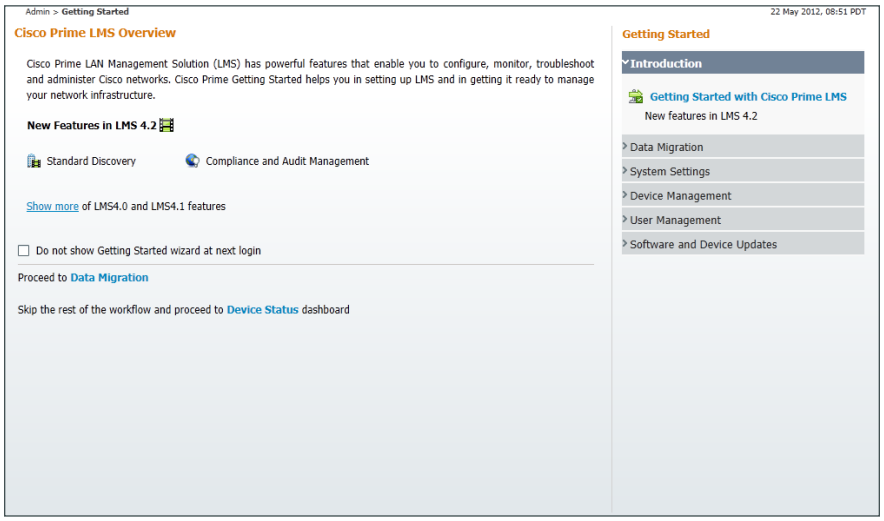
Step 3: Log in using the username **admin** and the password that you provided during installation.



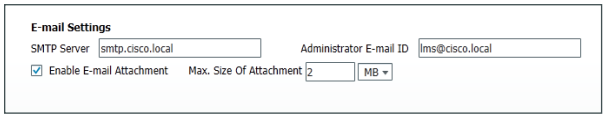
The Getting Started pane shows you the workflow for configuring Prime LMS.

Tech Tip

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



Step 4: Under Getting Started, click **System Settings**, enter values in the **SNTP Server** and **Administrator E-mail ID** field, and then click **Apply**. You will receive automatic email alerts about network issues, job status, report generation, etc.



Step 5: To configure the Prime LMS portal to support HTTPS connections, navigate to **Admin > Trust Management > Local Server > Browser-Server Security Mode Setup**.

Step 6: Select **Enable**, and then click **Apply**.

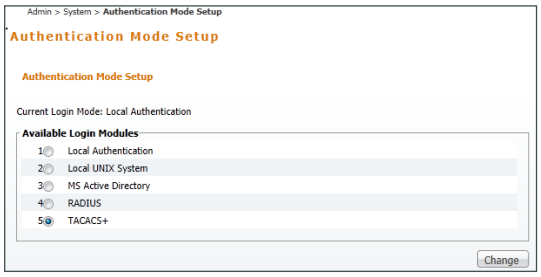
Procedure 4 Configure Prime LMS user authentication

(Optional)

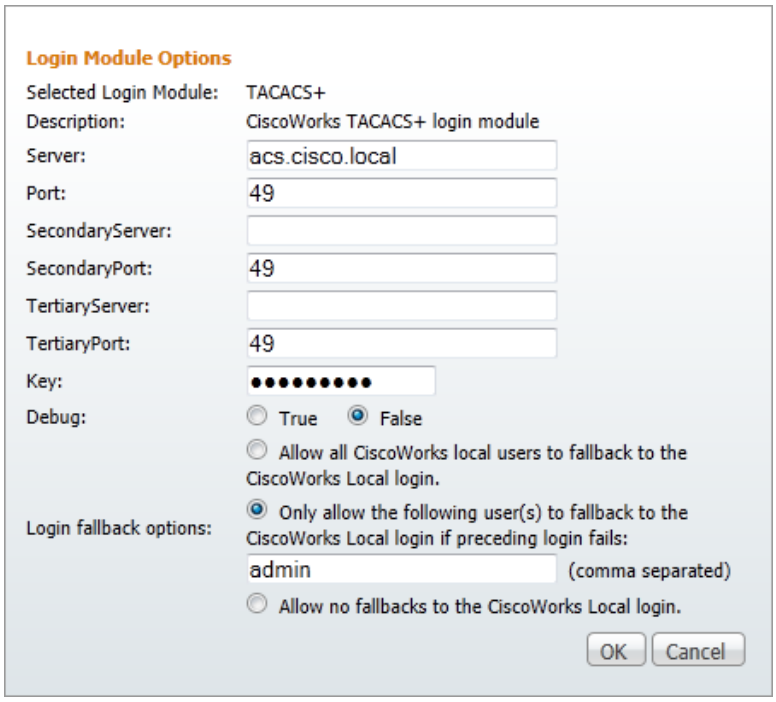
Prime LMS can use its local database, Active Directory, Lightweight Directory Access Protocol (LDAP), TACACS+, and many other modules to authenticate user logins. To enable a common authentication experience for network administrators across network devices and the network management system, this guide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

Step 1: Navigate to **Admin > System > Authentication Mode Setup**.

Step 2: Select **TACACS+**, and then click **Change**.



Step 3: Set the **Server** (Example: acs.cisco.local) and **Key** (Example: SecretKey), and then click **OK**.



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

Procedure 5 Configure Prime LMS user roles

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

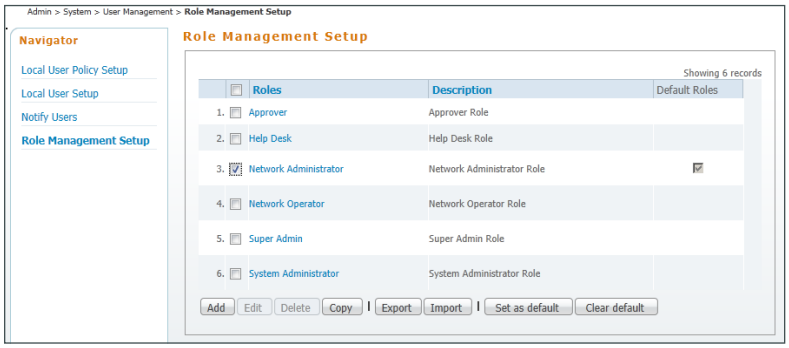
- **Help Desk**–These users can access network status information only. They cannot perform any action on a device or schedule a job on a network.
- **Network Operator**–Users can perform all help-desk tasks and tasks related to network data collection. They cannot perform any task that requires write-access 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 Prime LMS system administration tasks.
- **Super Admin**–Users can perform all Prime LMS operations, including administration and approval tasks.

When using an authentication module other than the Prime LMS local database, Prime LMS authenticates the user against the external module. After the user is successfully authenticated, Prime LMS assigns 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 use Prime LMS to perform network configuration tasks but not administer the Prime LMS system itself, assign Network Administrator as the default role.

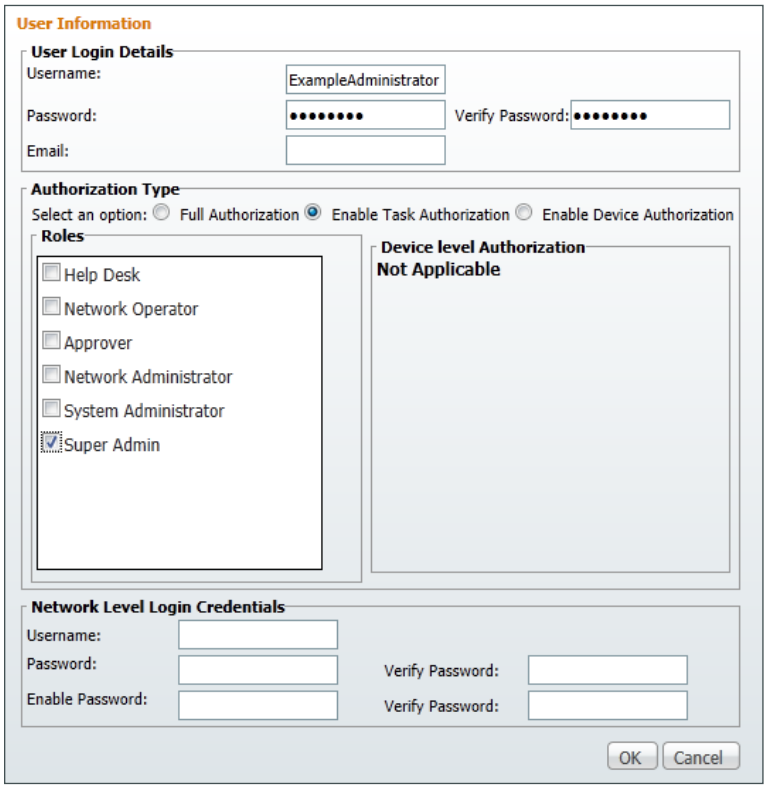


For any users who require different permissions than those included in the default role, create local user accounts and assign a Prime LMS role to each of the local user accounts you create.

Step 3: Navigate to **Admin > System > User Management > Local User Setup**.

Step 4: Click **Add**. The **Add Users** window opens.

Step 5: Enter the username used in the TACACS+ login, configure a password (it does not have to match the TACACS+ login password and it is not used during authentication), select the **Super Admin** check box, and then click **OK**.



Procedure 6 Add devices and credentials

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

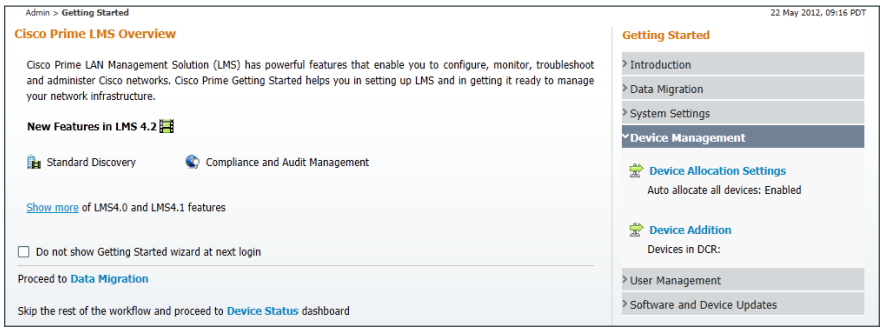
- Discover the devices using a discovery protocol
- Add devices manually
- Bulk import of devices

Prime LMS supports Layer 2 and Layer 3 protocols for device discovery. Device discovery using Cisco Discovery Protocol is the preferred protocol used by Prime LMS to discover network devices in the LAN.

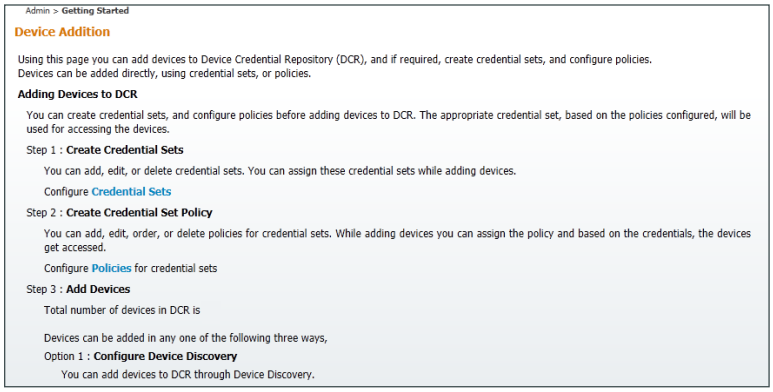
Both Cisco Discovery Protocol and SNMP must be enabled on devices before using this procedure. If you did not deploy your network by using the CVD design guides, which enable both of these protocols, see http://cisco.com/go/lms for guidance.

The example presented here uses the Prime LMS Discovery feature.

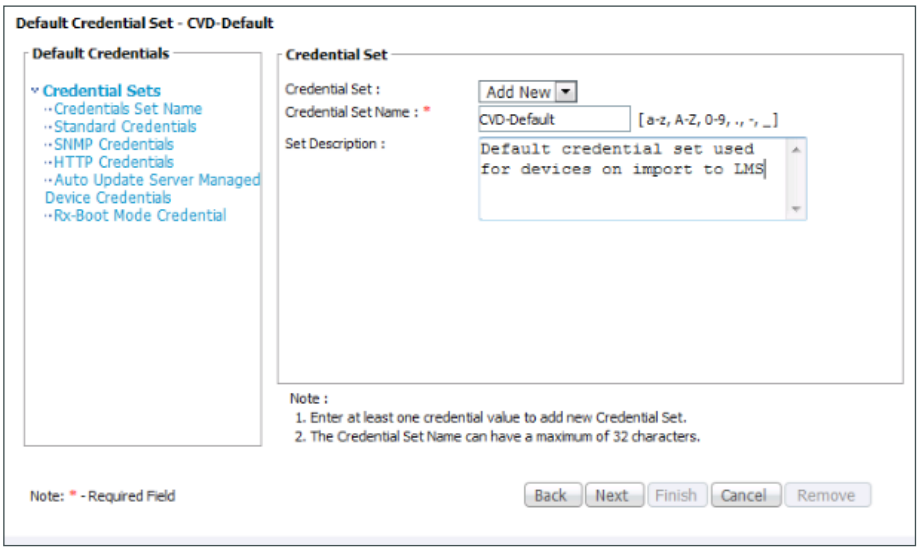
Step 1: Navigate to **Admin > Getting Started > Device Management > Device Addition**.



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

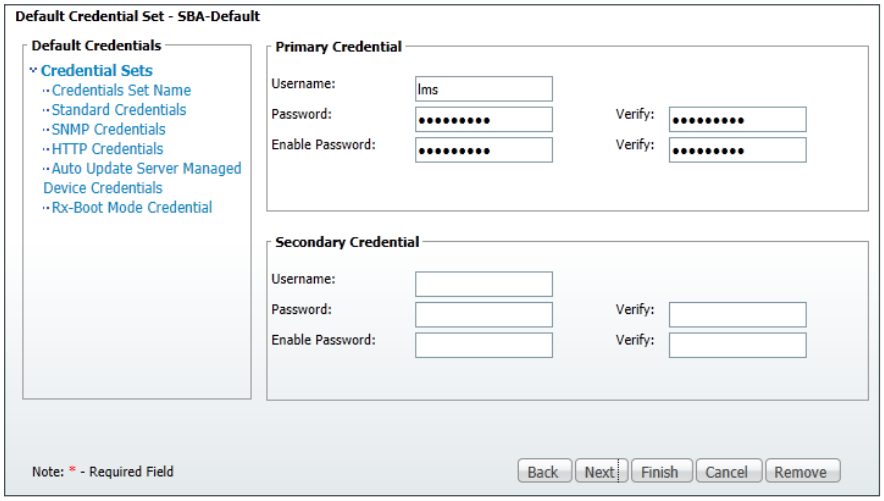


Step 3: Click **Credential Set Name**, and then set the **Credential Set Name** to **CVD-Default**.

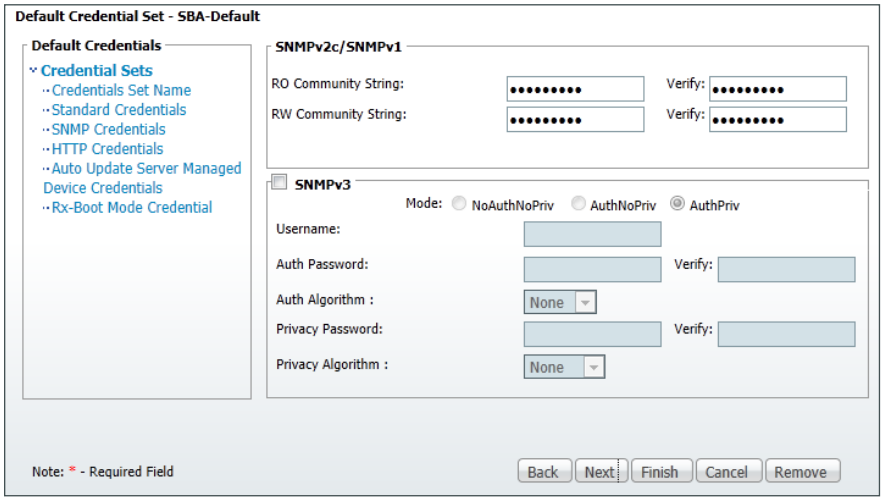


Step 4: Click **Next**.

Step 5: In **Standard Credentials**, enter the **Username** (Example: lms), **Password**, and **Enable Password** that Prime LMS should use when logging in via SSH, and then click **Next**.

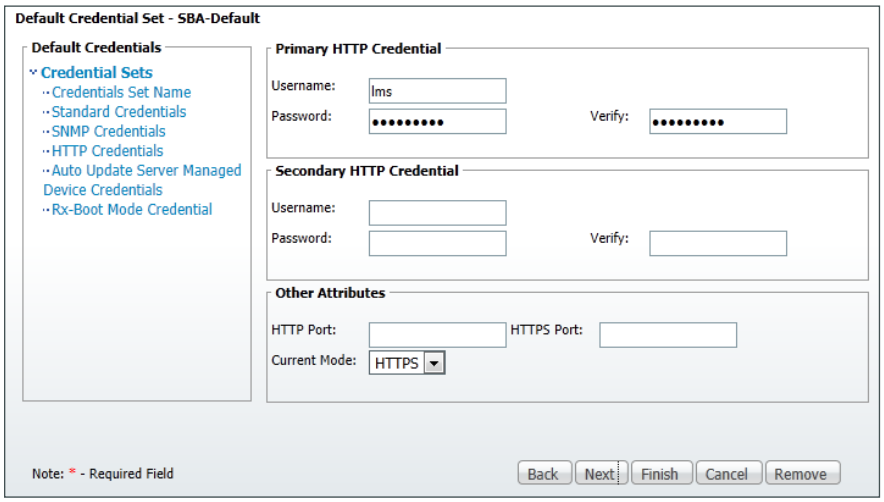


Step 6: In **SNMP Credentials**, configure the **RO Community String** (Example: cisco) and **RW Community String** (Example: cisco123) that Prime LMS should use to poll the network devices, and then click **Next**.

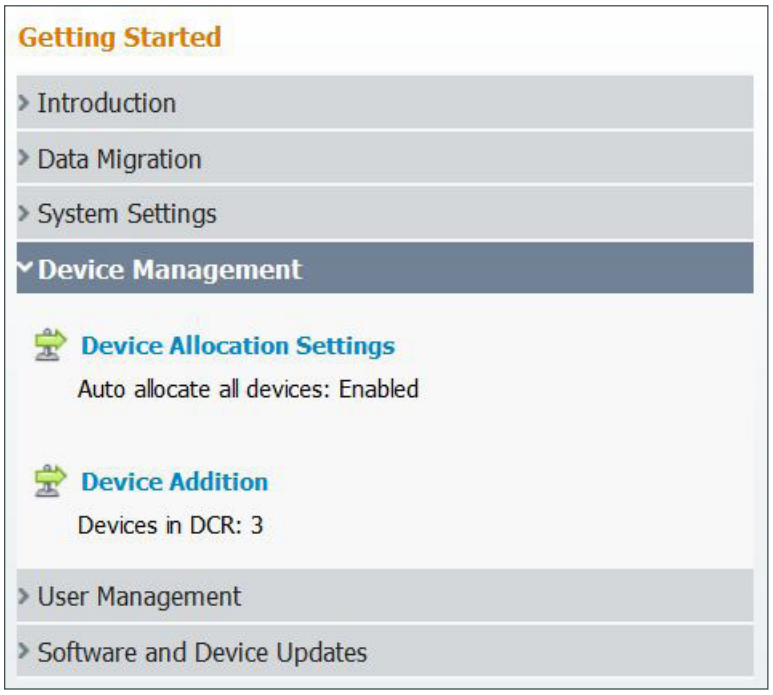


Step 7: In **HTTP Credentials**, configure the **Username** (Example: lms) and **Password** that Prime LMS should use when configuring a device via HTTPS.

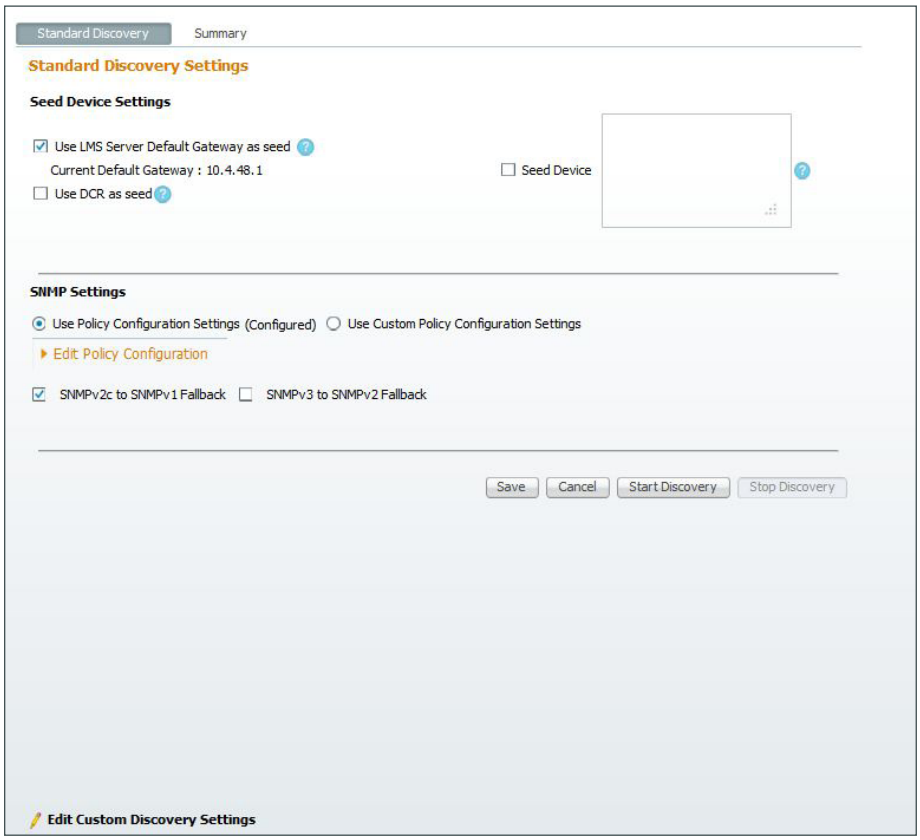
Step 8: In the **Current Mode** list, choose **HTTPS**, and then click **Finish**.



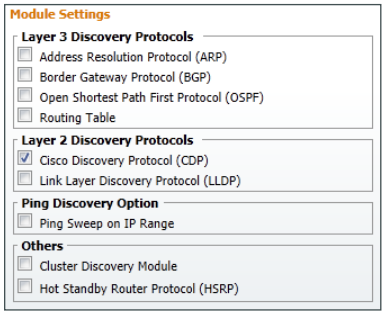
Step 9: On **the Admin > Getting Started** page, click **Device Management**. The Module Settings pane appears. You use this pane to enable the discovery protocols that Prime LMS will use to discover the devices on the network.



Step 10: **Select Device Addition**, then scroll down to **Edit Custom Discovery Settings**.



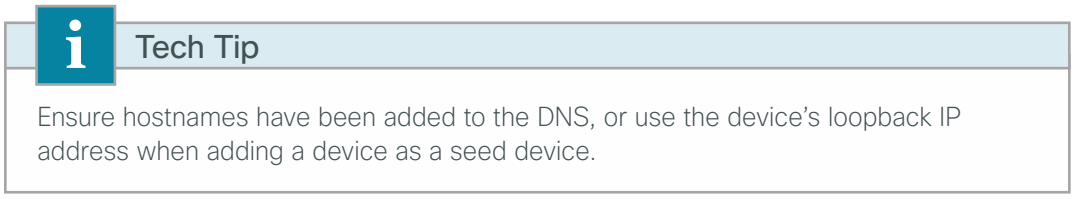
Step 11: Select **Cisco Discovery Protocol**, and then click **Next**.



The seed device setting page appears. A seed device is the start point from which Prime LMS discovers the network. The seed devices should be the core devices on the network and should reside in DNS. The Campus Wired LAN Design Guide presents core device options for a range of performance and scale scenarios.

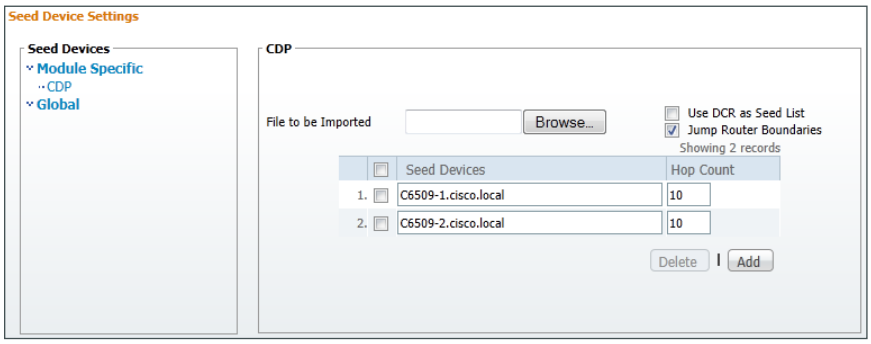
Step 12: Click **CDP**, click **Add**, and then configure the first seed device as the LAN core switch (Example: C6509-1.cisco.local). Enter the maximum number of hops under **Hop Count** for the first device.

Step 13: Click **Add** again, configure the second seed device as the other core switch (Example: C6509-2.cisco.local), enter the maximum number of hops under Hop Count for the second device, and then click **Next**.



Tech Tip

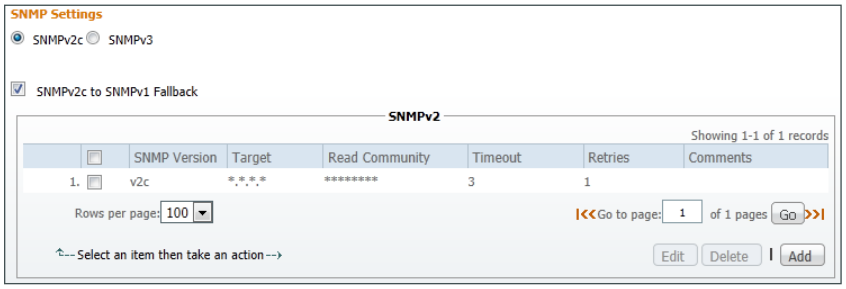
Ensure hostnames have been added to the DNS, or use the device's loopback IP address when adding a device as a seed device.



Step 14: On the **SNMP settings configuration** page, click **Add**. A new window pops up.

Step 15: Enter the target value (*.*.*.*), which tells Prime LMS to use this SNMP community string for all devices during discovery.

Step 16: Enter the read-only SNMP community string configured on your network devices (Example: cisco), and then click **OK**.

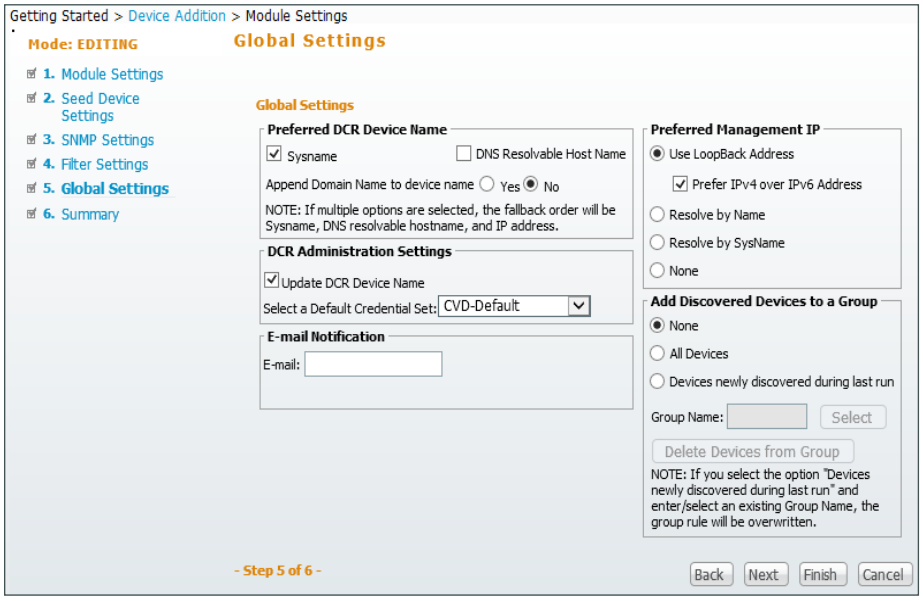


Step 17: Click **Next** for **Global Settings**, and under Preferred DCR Display Name, select **Host Name**.

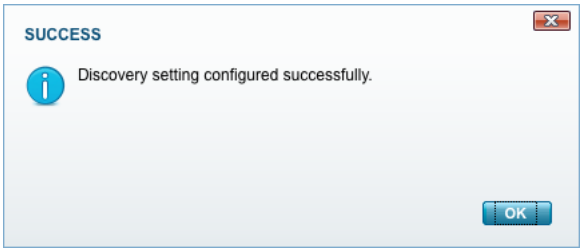
Step 18: Select **Update DCR Display Name**.

Step 19: In the **Default Credential Set** list, choose **CVD-Default**.

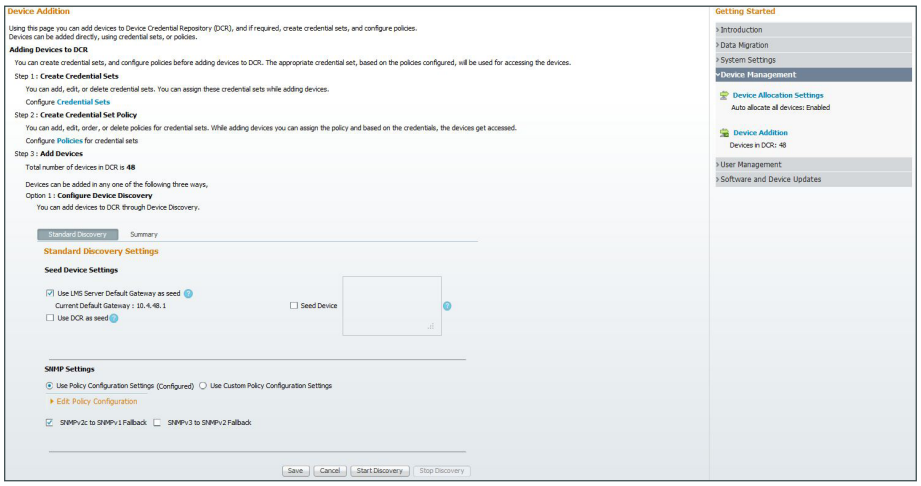
Step 20: Under Preferred Management IP, select **Use LoopBack Address**, check **Prefer IPv4 over IPv6 Address**, and then click **Finish**.



Step 21: In the message that informs you that discovery settings are successfully configured, click **OK**.

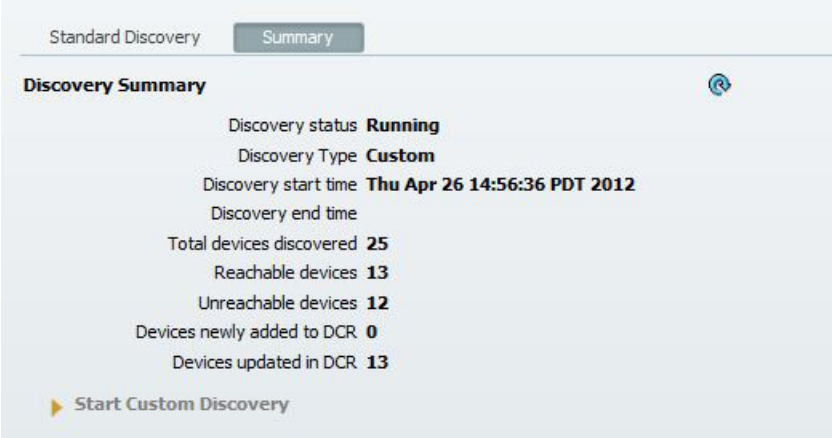


Step 22: Near the bottom of the Adding Devices to DCR page, click **Start Discovery**.

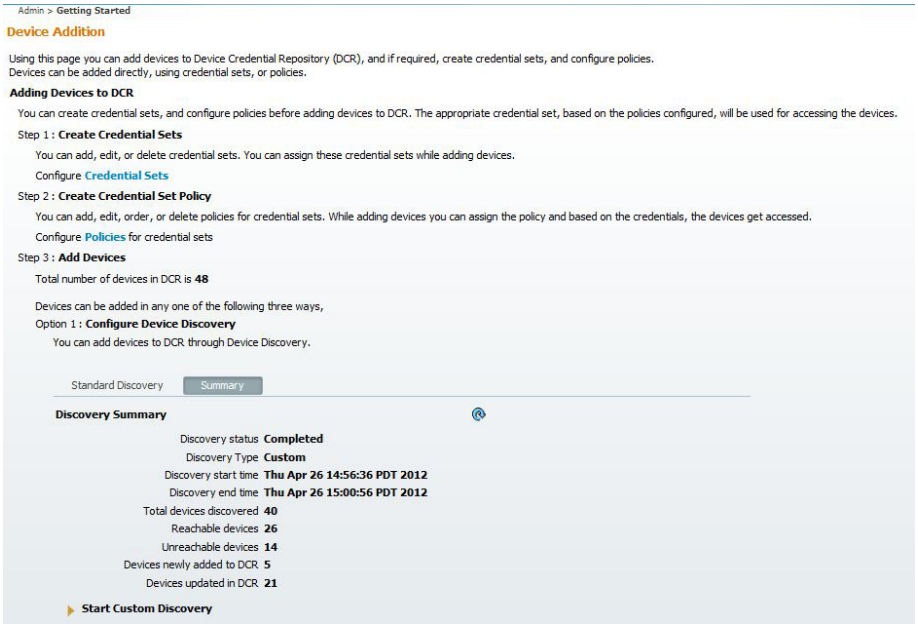


Prime LMS starts discovering the devices on the network. The amount of time this discovery process takes depends on the number of devices on the network. The Discovery window is refreshed every 5 seconds and updates the number of devices being discovered.

Step 23: If you want to view the discovery progress, click the discovery **Summary** tab. The data automatically updates. If you want to instantly update the in-progress results, click the blue refresh icon.



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



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

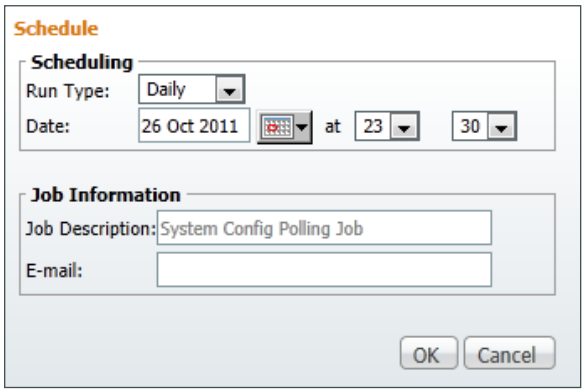
Device configuration can occur on an as-needed or scheduled basis.

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

Step 2: Click **Config Collection Settings**, and then under Period Polling, select **Enable**.

Step 3: Click **Schedule**.

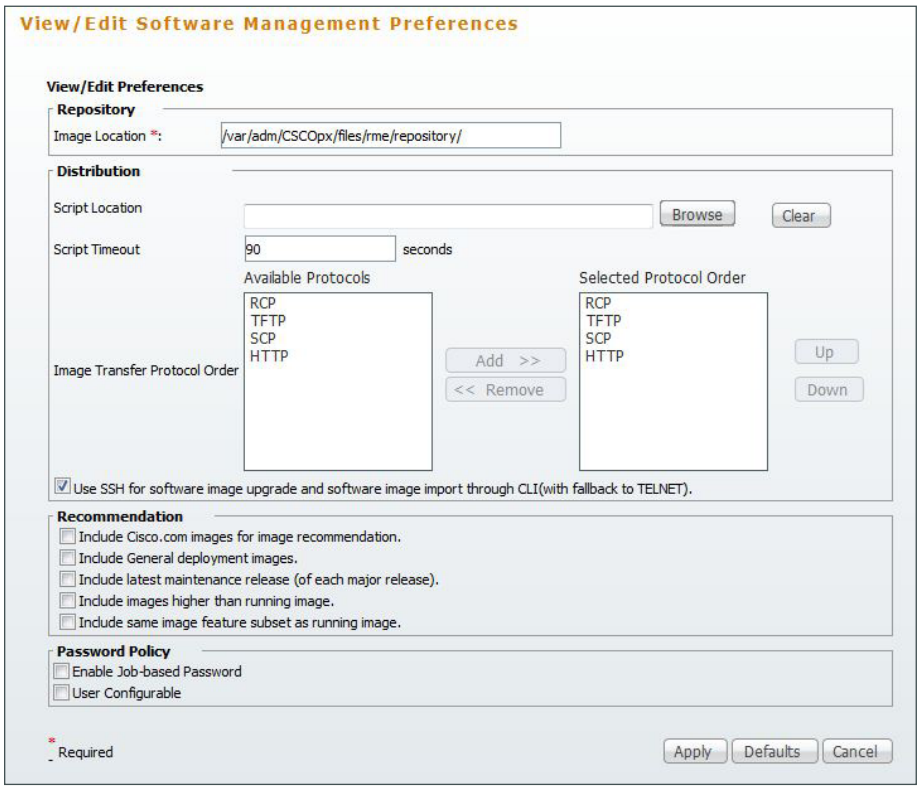
Step 4: In the window that appears, set the time to a non-peak time on the network, and then click **OK**.



Step 5: Click **Apply**.

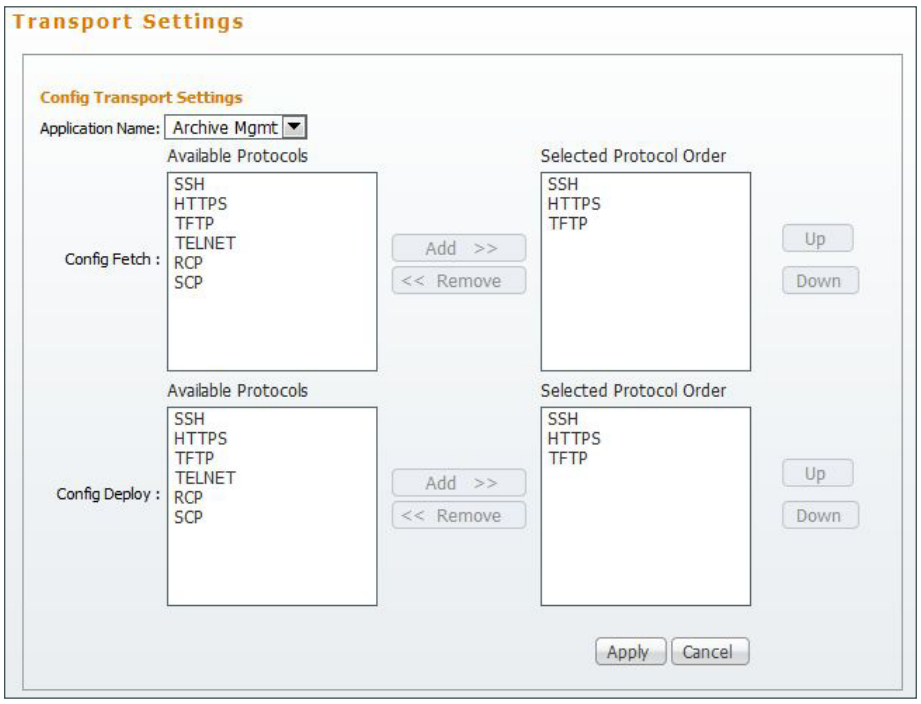
Step 6: Repeat Step 2 through Step 5 for Periodic Collection.

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**.



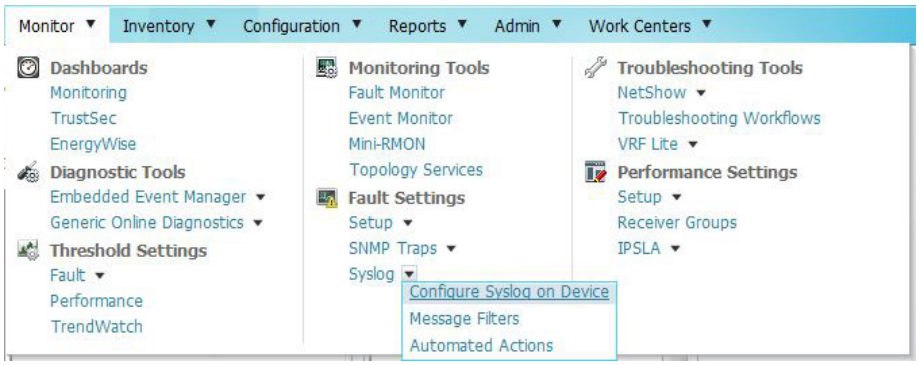
Step 8: Navigate to **Admin > Collection Settings > Config > Config Transport Settings**.

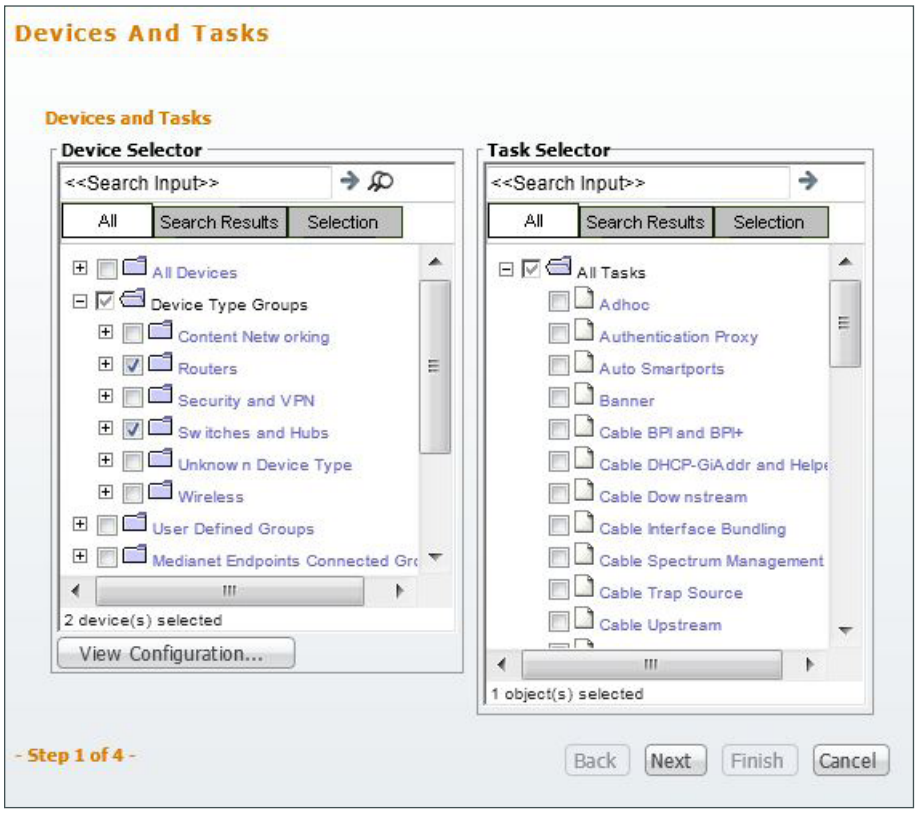
Step 9: For each application in the **Application Name** list, adjust the selected protocol order to be **SSH**, **HTTPS**, **TFTP**, and then click **Apply**.



Procedure 8 Configure syslog collection

Step 1: Navigate to **Monitor > Fault Settings > Syslog > Configure Syslog on Device**. The screen **Devices and Tasks** appears.





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

Step 3: Select **Routers**.

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

Step 5: Click **Add Instance**.

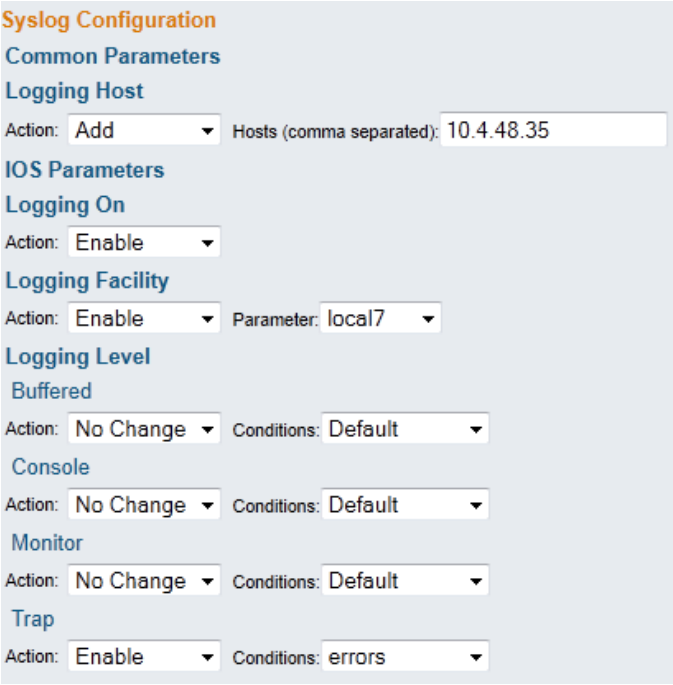
Step 6: Set the **Logging Host Action** to **Add** and set **Hosts** to the Prime LMS server (10.4.48.35).

Step 7: Set the **Logging On Action** to **Enable**.

Step 8: Set the **Logging Facility Action** to **Enable** and the **Parameter** to **local7**.

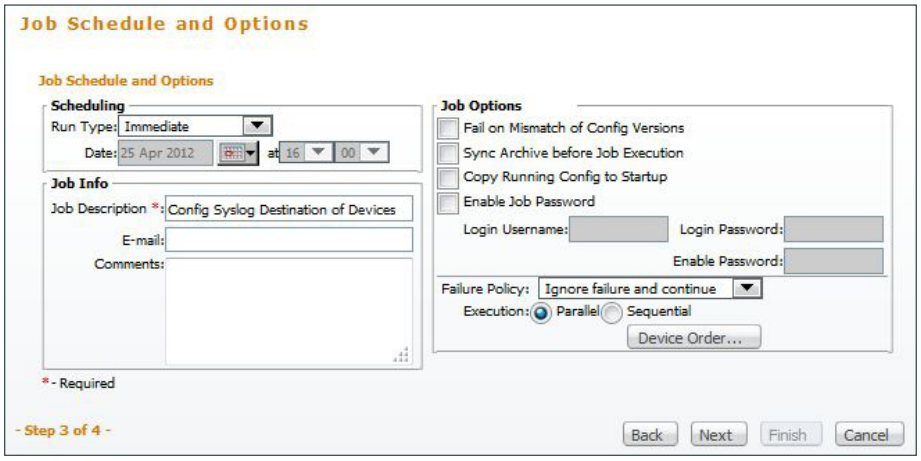
Step 9: Set the **Trap Action** to **Enable** and the **Conditions** to **errors**.

Step 10: Click **Save**.



Step 11: Click **Next**.

Step 12: Enter **Job Description** (Example: Configure Syslog Destination of Devices), and then click **Next**.



Step 13: At the Job Work Order screen, click **Finish**.

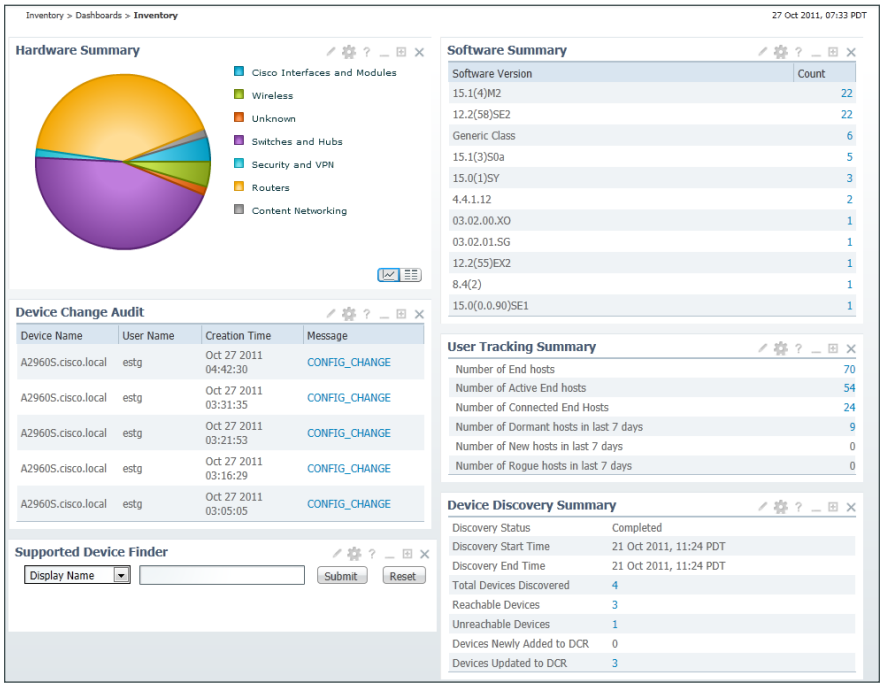
Step 14: Click **Monitor**. You can now view the syslog messages.

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.

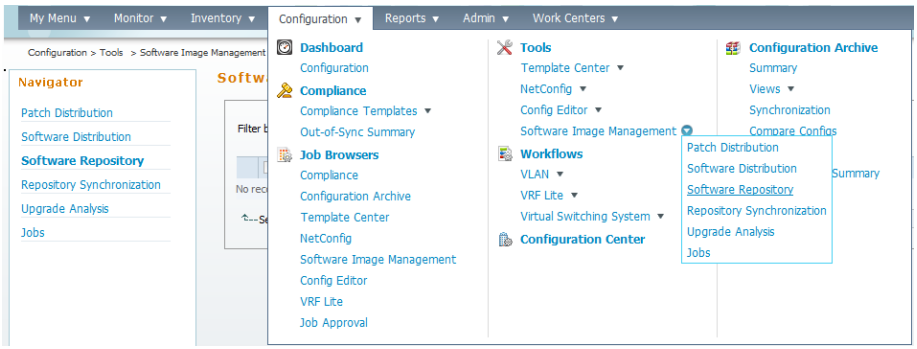


Procedure 1 Distribute software images

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 Prime LMS local software image repository or on cisco.com. Available upgrade options are shown, and Prime LMS allows you to upgrade a managed device to an image through the GUI.

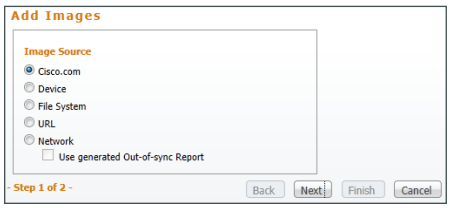
You can add software images to the repository (from cisco.com or a device, file system, or URL).

Step 1: Navigate to **Configuration > Tools > Software Image Management > Software Repository**.



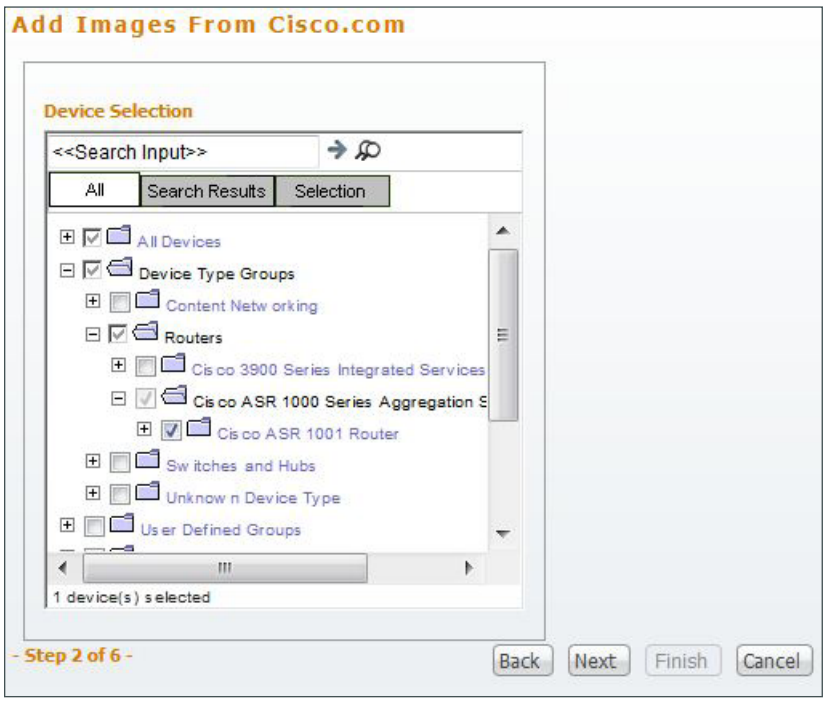
Step 2: Click **Add**.

Step 3: Choose the source (Example: cisco.com) from which to you want to acquire the image, and then click **Next**.



Next you must select device(s) for software upgrade.

Step 4: In the Prime LMS inventory, select a device, and then click **Next**.

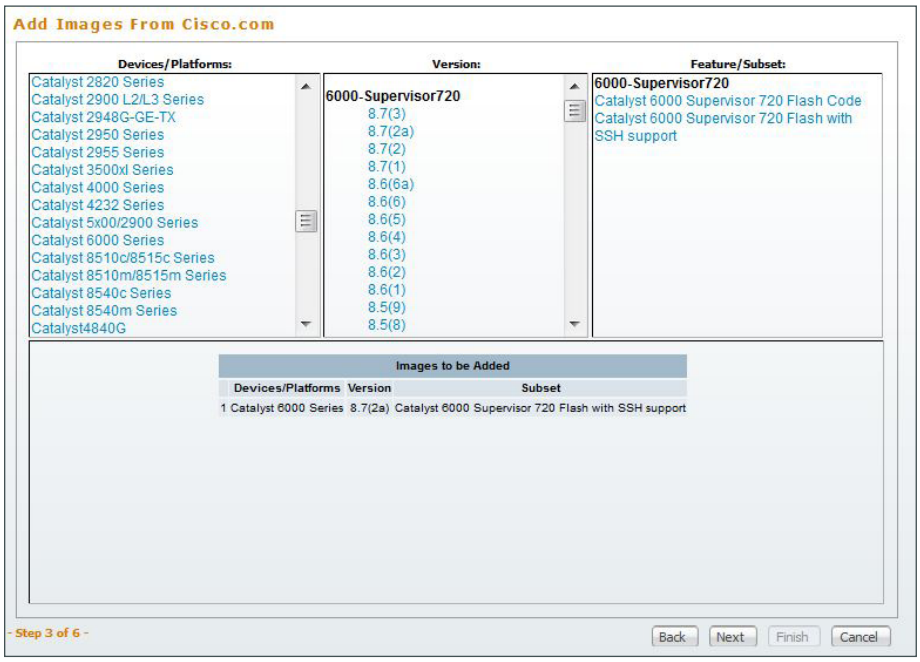


Step 5: In the **Device/Platforms** pane, click the device name.

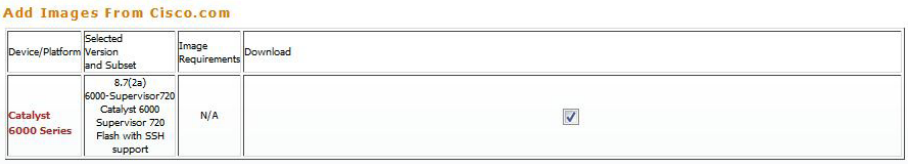
Step 6: In the **Version** pane, select the Software Version.

Step 7: In the **Feature/Subset** pane, select the Software Feature Set.

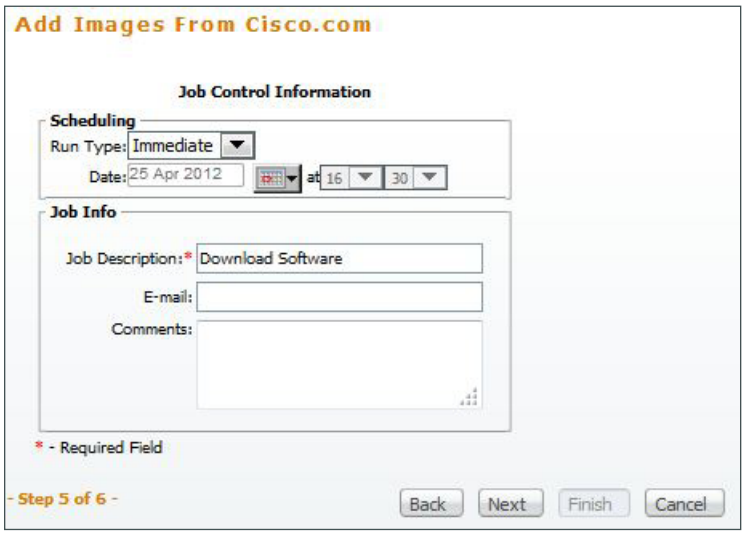
Step 8: Click **Next**.



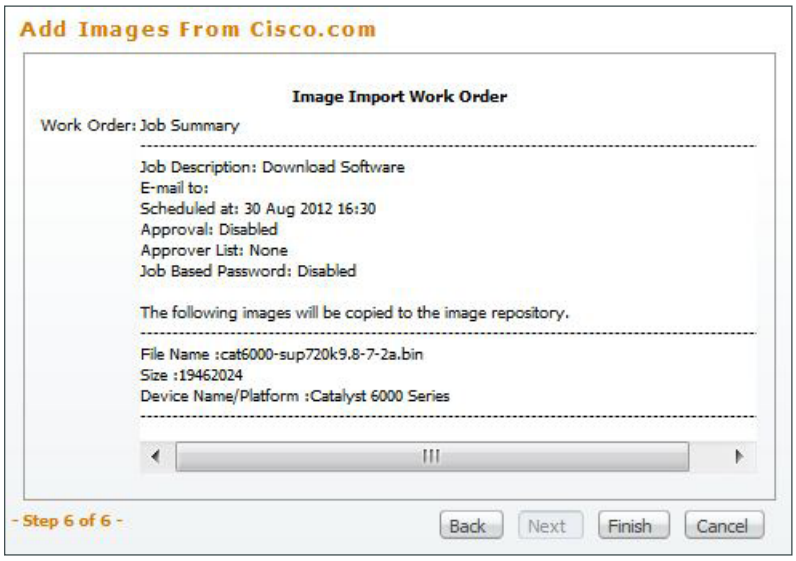
Step 9: Ensure that the check box in the Download column is selected, and then click **Next**.



Step 10: Enter a Job Description, and then click **Next**.



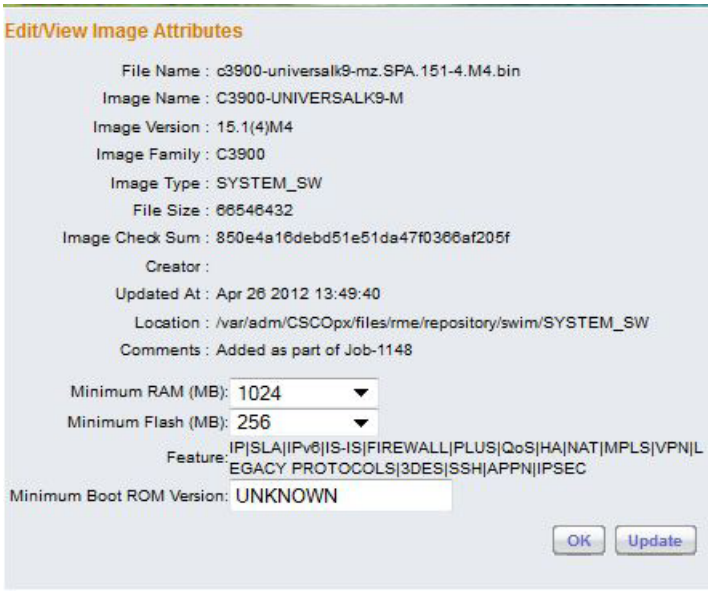
Step 11: On the **Image Import Work Order**, view the software image job summary, and then click **Next**.



Step 12: Click **Finish**.

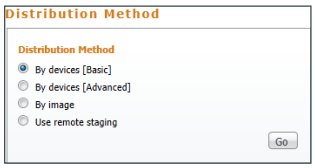
Step 13: Click the name of the software image that was added in the previous step and make sure that the device requirements are set correctly.

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

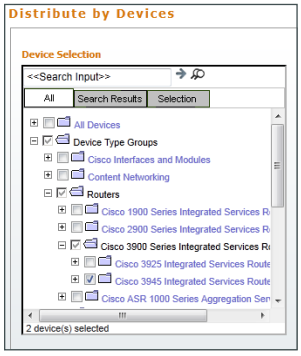


Step 15: Navigate to **Configuration > Tools > Software Image Management > Software Distribution**.

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

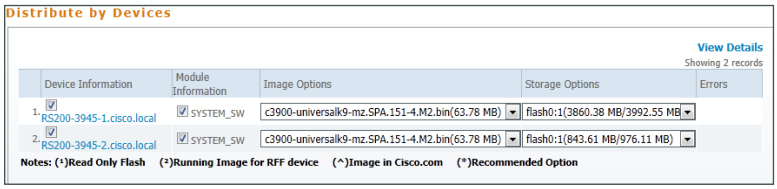


Step 17: Choose the device or devices for software image distribution, and then click **Next**.



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

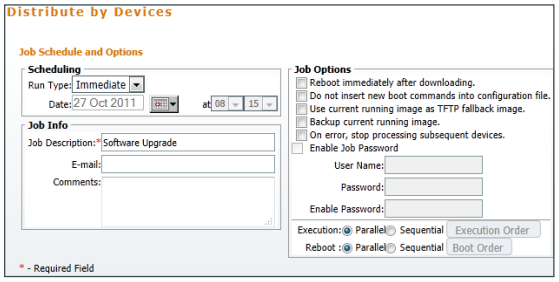
Prime LMS shows the images available in the software repository for the selected device or devices.



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

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

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



A new page shows the work order that was just created.

Step 22: Click **Finish**. This completes the work order.

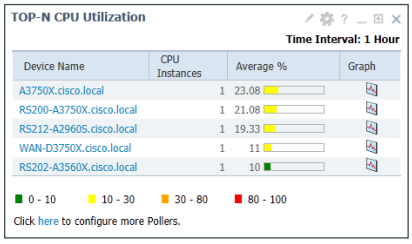
Procedure 2 Customize monitoring

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. Prime 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.

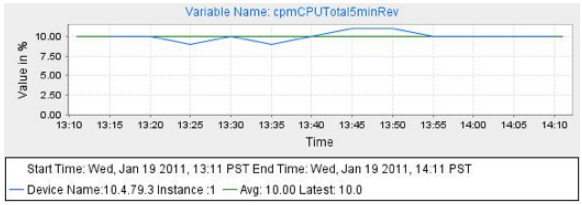
You can customize these activities based on your network needs. This procedure describes one such activity, CPU utilization.

Step 1: Access the Monitoring Dashboard by navigating to **Monitor > Dashboards > Monitoring**.

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



Step 2: Click the **Graph** icon. This displays the details of the CPU utilization for a specific device.

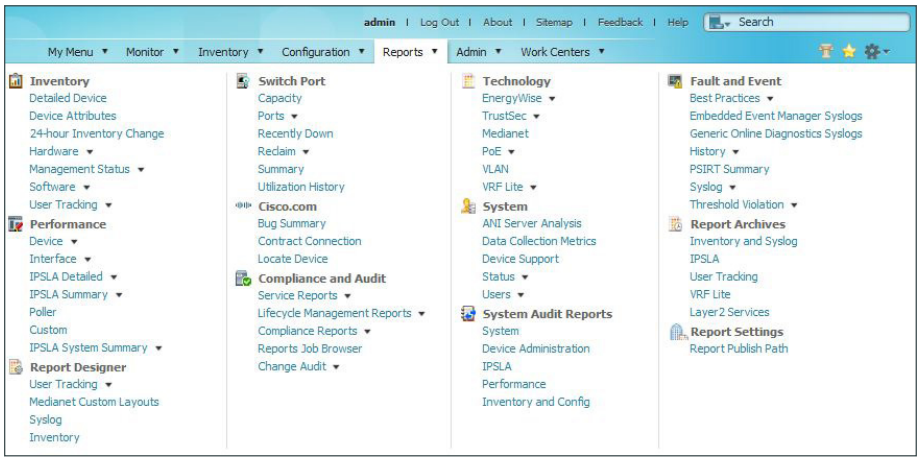


Procedure 3 Generate and view reports

Prime 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
- **System Audit**—Contains audit reports for software image distribution and download history
- **Report Designer**—Generates custom reports, especially for syslog and inventory

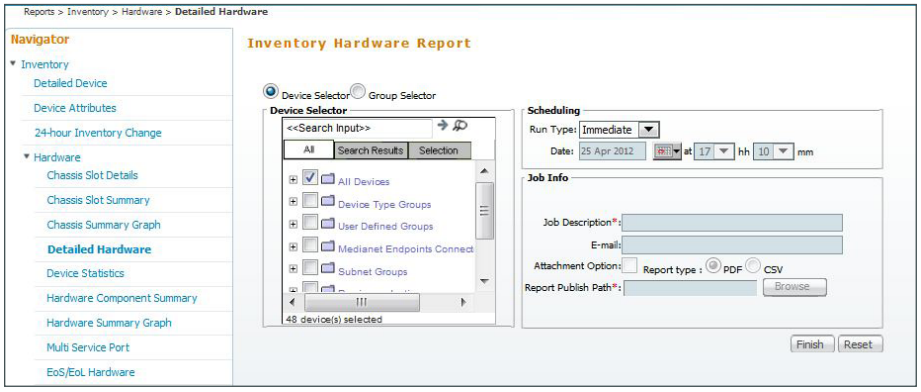
- **cisco.com**–Allows you to check contract information and bug status by using the bug toolkit
- **Compliance and Audit**–Reports status of all services on the network, lifecycle management, and regulatory compliance such as HIPAA, SOX, etc.
- **View Report Archives**–Creates a report from a scheduled report and stores it in the 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**.



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

Cisco Catalyst 6500 Series Switches

Device Name	Updated At	System Description	Location	Contact	Serial Number	Chassis Vendor Type	Total RAM Size(MB)	NVRAM Size (KB)	NVRAM Used (KB)	ROM Version	Total Flash Device Size (MB)
6509-1	Apr 24 2012 16:26:46	Cisco IOS Software, s2t54 Software (s2t54-IPSERVICESK9-M), Version 15.0(1)SY1, RELEASE SOFTWARE (fc4) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by Cisco Systems, Inc. Compiled Thu 16-Feb-12 21:36 by prod_rel_team			SMG1233N2S7	cevChassisCat6509	1024.00	0.00		12.2(50r)SYS	3938.28
C6509-2.cisco.local	Apr 25 2012 12:02:04	Cisco IOS Software, s2t54 Software (s2t54-IPSERVICESK9-M), Version 15.0(1)SY1, RELEASE SOFTWARE (fc4) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by Cisco Systems, Inc. Compiled Thu 16-Feb-12 21:36 by prod_rel_team			SMG1233N2S9	cevChassisCat6509	1024.00	0.00		12.2(50r)SYS	21495.96
C6509-1.cisco.local	Apr 25 2012 12:02:14	Cisco IOS Software, s2t54 Software (s2t54-IPSERVICESK9-M), Version 15.0(1)SY1, RELEASE SOFTWARE (fc4) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by Cisco Systems, Inc. Compiled Thu 16-Feb-12 21:36 by prod_rel_team			SMG1233N2S7	cevChassisCat6509	1024.00	0.00		12.2(50r)SYS	3938.28

Cisco Catalyst 3750 Series Switches

Device Name	Updated At	System Description	Location	Contact	Serial Number	Chassis Vendor Type	Total RAM Size(MB)	NVRAM Size (KB)	NVRAM Used (KB)	Total Flash Device Size (MB)
HQ-C3750X-PR1.cisco.local	Apr 25 2012 12:03:20	Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version 15.0(1)SE2, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled Thu 22-Dec-11 00:05 by prod_rel_team			FDO1443Z10Y	cevChassisWsC3750x24P	272.00	512.00	26.35	55.00

Procedure 4 Deploy templates

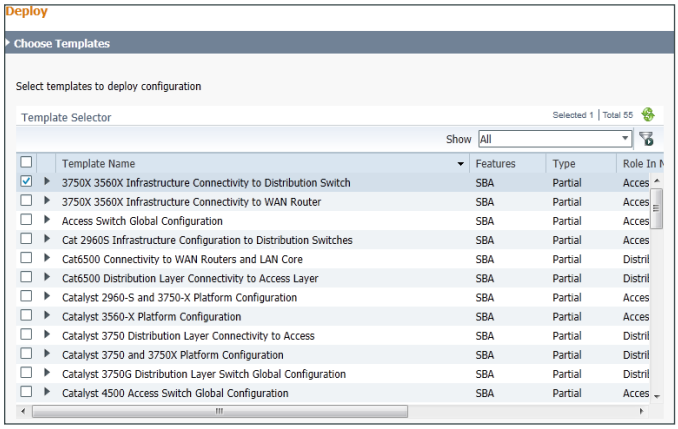
Another important feature, *templates*, is specifically designed for deploying configurations in managed networks. Typically, a network consists of thousands of devices, and it is an enormous task for administrators to configure each of these devices individually. Ideally, they would like to have a set 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 Prime 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 the CVD architecture.

Templates based on Campus Wired LAN Design Guide are included as part of Cisco Prime 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.

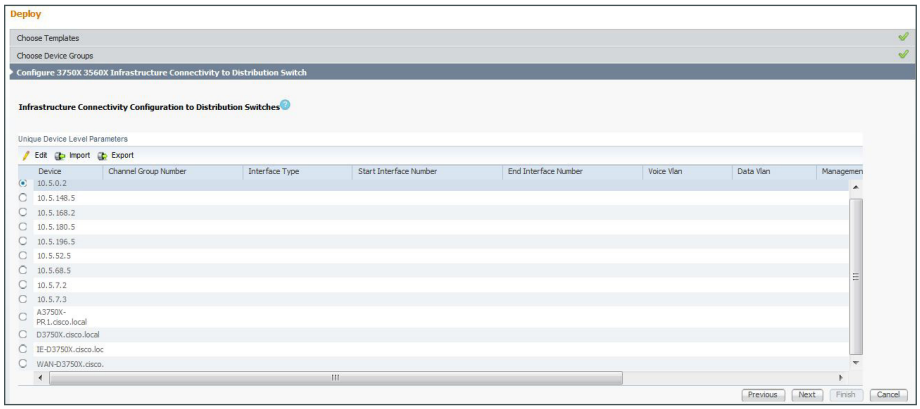
Step 1: In the Prime LMS portal, navigate to **Configuration > Template Center**. The Deploy screen appears.

Step 2: Choose the template that you would like to deploy, and then click **Next**. You can sort how the templates are displayed by clicking the column titles.



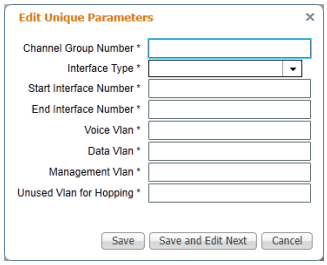
Step 3: In Device Selector, choose the devices to which you want to push these templates, and then click **Next**.

Step 4: In the list, choose to which device in the network you want to apply the configuration.

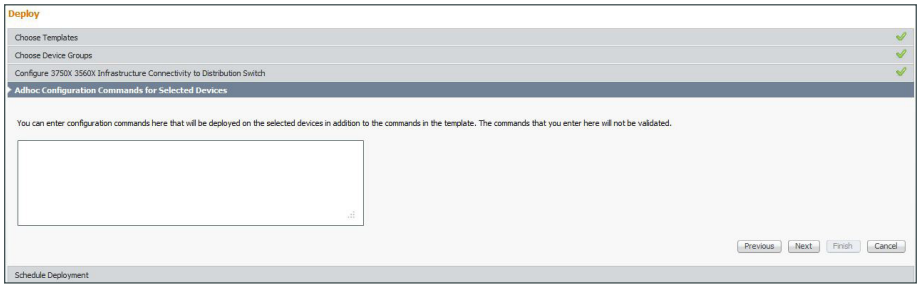


A page appears that requires you to provide the variables for the commands for that particular template. In this example, LAN Switch Universal Template displays the required variables.

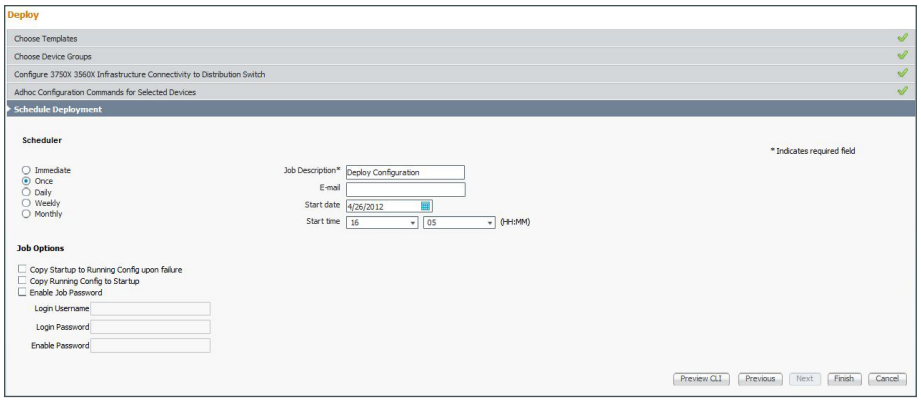
Step 5: Fill in the required variables, and then click **Save and Edit Next**.



Step 6: The Ad Hoc Configuration Commands for Selected Devices page lets you enter configuration commands that will be deployed on the selected devices in addition to the commands in the template.



Step 7: Enter the desired deployment frequency and date(s), a Job Description, and then click **Finish**. This deploys the template on the selected device based on the scheduled settings. If you choose the email option, Prime LMS sends a confirmation email to the specified administrator.



Appendix A: Product List

Network Management

Functional Area	Product Description	Part Numbers	Software
Network Management	Cisco Prime Infrastructure 1.1	R-PI-1.1-K9	4.2
	Prime Infrastructure 1.1 Software - 10K Device License	R-PI-1.1-10K-K9	
	Prime Infrastructure 1.1 Software – 5K Device Base License	R-PI-1.1-5K-K9	
	Prime Infrastructure 1.1 Software – 2.5K Device Base License	R-PI-1.1-2.5K-K9	
	Prime Infrastructure 1.1 Software – 1K Device Base License	R-PI-1.1-1K-K9	
	Prime Infrastructure 1.1 Software – 500 Device Base License	R-PI-1.1-500-K9	
	Prime Infrastructure 1.1 Software – 100 Device Base License	R-PI-1.1-100-K9	

Feedback

Please use the feedback form to send comments and suggestions about this guide.

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.

B-0000270-1 08/13