



Prime Infrastructure

Technology Design Guide

August 2014 Series



Table of Contents

| | |
|--|-----------|
| Preface | 1 |
| CVD Navigator | 2 |
| Use Cases | 2 |
| Scope | 2 |
| Proficiency..... | 2 |
| Introduction | 3 |
| Technology Use Case | 3 |
| Use Case: Managing Network Devices | 3 |
| Design Overview..... | 3 |
| Device Work Center | 5 |
| Configuration Templates and Tasks | 5 |
| Alarms, Events, and Syslog Messages | 5 |
| Reporting..... | 6 |
| More About Cisco Prime Infrastructure..... | 6 |
| Deployment Details | 7 |
| Installing and Configuring Cisco Prime Infrastructure..... | 7 |
| Managing the Network | 29 |
| Appendix A: Product List | 40 |
| Appendix B: Changes | 41 |

Preface

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

CVDs include two guide types that provide tested design 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 existing CVDs but also include product features and functionality across Cisco products and sometimes 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.

CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit [the CVD Foundation web site](#).

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

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 Network Devices**—The network management needs of administrators include configuration backup and archive; configuration deployment; software image management; and monitoring, troubleshooting, and reporting of events on managed devices.

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

Scope

This guide covers the installation, set up, and basic operation of Cisco Prime Infrastructure.

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



Campus Wireless LAN
Technology Design Guide



Campus CleanAir Technology
Design Guide

To view the related CVD guides, click the titles or visit [the CVD Foundation web site](#).

Introduction

Cisco Prime Infrastructure is a network management application capable of managing up to 18,000 devices of various types, including LAN and WAN devices. This CVD guide describes the operational challenges that Cisco Prime Infrastructure can help organizations resolve and provides procedures for installing and using some of the essential network management features.

Technology Use Case

As networks and the number of services they support continue to evolve, the responsibilities of network administrators to maintain and improve their efficiency and productivity also grow. Using a network management solution can enable and enhance the operational efficiency of network administrators.

Use Case: Managing Network Devices

Network administrators have a demanding, tedious job overseeing all the devices on a network. To complicate matters, network devices are sometimes added to or removed from the network. As an organization grows, so too does the number of devices to be managed.

The network management needs of administrators include:

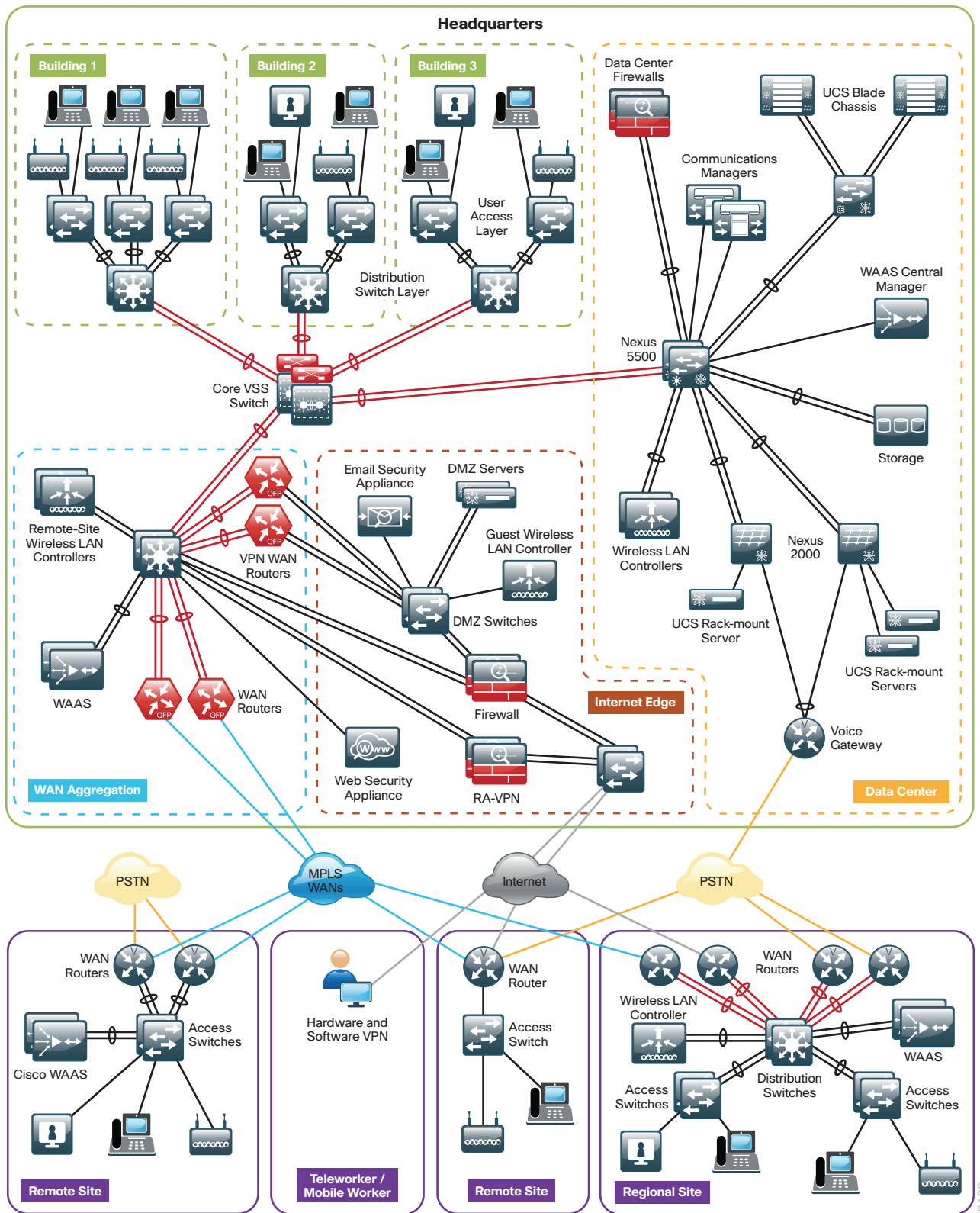
- **Configuration backup and archive**—Administrators need to make backup copies of device configurations and store them in a protected location. Performing this task manually is extremely time-consuming and tedious. An automated means of collecting and archiving device configuration files is an invaluable aid to network administrators.
- **Configuration deployment**—When a change in the network or in the services it supports requires changes to device configurations, manually connecting to and configuring all affected devices can take many hours, just to make similar—if not identical—changes to device configurations. A means of automating the deployment of such configuration changes, including support for device-specific values, can greatly improve the speed and also the accuracy of updating the network.
- **Software image management**—A centralized way of viewing the operating system versions running on all network devices is very helpful but administrators also need the ability to get necessary software images from a trusted source and then to propagate images to many network devices.
- **Monitoring, troubleshooting, and reporting**—Running a network requires knowing the state of the network and the state of individual devices. It also requires notification of events on the network, troubleshooting tools, and an ability to generate reports about many aspects of the network.

Design Overview

Cisco Prime Infrastructure is a sophisticated network management tool that can help support the end-to-end management of network technologies and services that are critical to the operation of your organization; it aligns network management functionality with the way that network administrators do their jobs. Cisco Prime Infrastructure provides an intuitive, web-based GUI that can be accessed from anywhere from within the network and gives you a full view of a network use and performance.

Figure 1 depicts the campus network architecture documented in the [Campus Wired LAN Technology Design Guide](#) and [Campus Wireless LAN Technology Design Guide](#). With such a network and the services that it can support, Cisco Prime Infrastructure can play a critical role in day-to-day network operations.

Figure 1 - Campus Wired and Wireless LAN Architecture



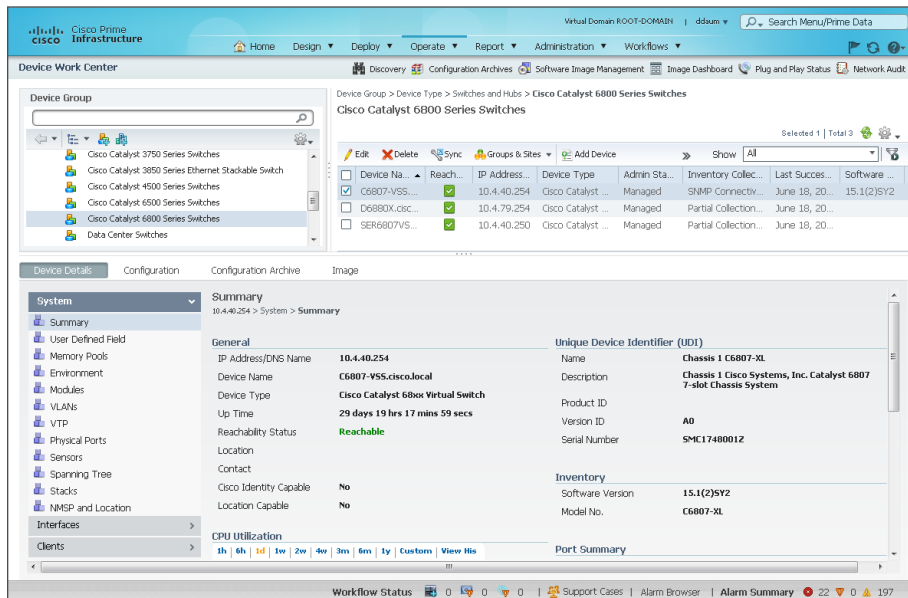
2189

Device Work Center

Cisco Prime Infrastructure includes the Device Work Center. Some of the features found in the Device Work Center are:

- **Discovery**—Builds and maintains an up-to-date inventory of managed devices, including software image information and device configuration details.
- **Configuration Archives**—Maintains an active archive of multiple iterations of configuration files for every managed device.
- **Software Image Management**—Enables a network administrator to import software images from Cisco.com, managed devices, URLs, or file systems, and then distribute them to a single device or group of devices.

Figure 2 - Device Work Center



Configuration Templates and Tasks

Using the Configuration Tasks feature to apply configuration templates to many devices, administrators can save many hours of work. Cisco Prime Infrastructure provides a set of command-line interface (CLI) templates and you can use them to create a configuration task, providing device-specific values as needed.

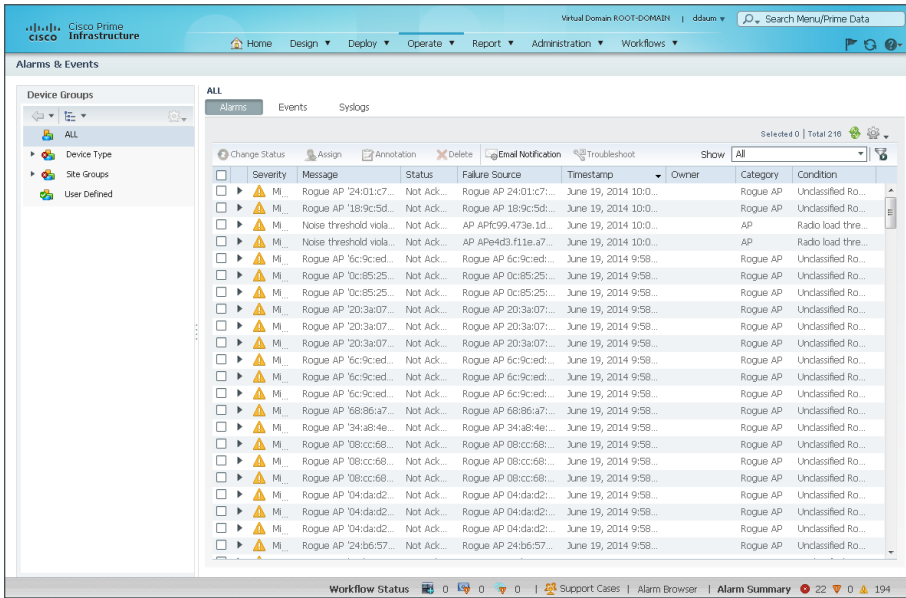
For other configuration needs, Cisco Prime Infrastructure enables you to define your own templates with Apache Velocity Template Language (VTL). For more information about Apache VTL, see:

<http://velocity.apache.org/engine/devel/vtl-reference-guide.html>

Alarms, Events, and Syslog Messages

Cisco Prime Infrastructure provides the Alarms and Events feature, which is a unified display with detailed forensics. The feature provides actionable information and the ability to automatically open service requests with the Cisco Technical Assistance Center (TAC).

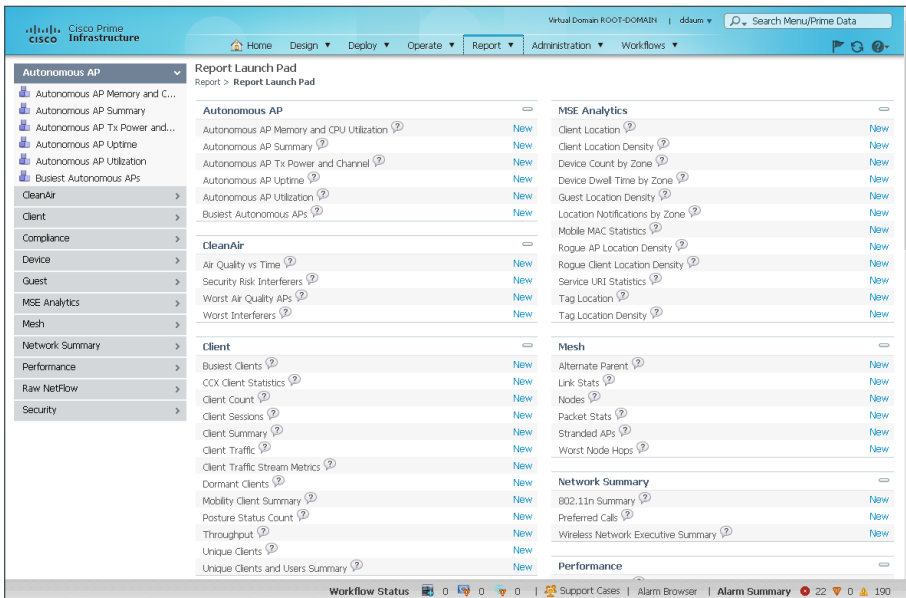
Figure 3 - Alarms and Events



Reporting

Cisco Prime Infrastructure provides you a single launch point for all reports that you can configure, schedule, and view. The Report Launch Pad page provides access to over 100 reports, each of which you can customize as needed.

Figure 4 - Report Launch Pad



More About Cisco Prime Infrastructure

Cisco Prime Infrastructure provides many features and capabilities that are outside the focus of this CVD guide. For more information about Cisco Prime Infrastructure, visit:

<http://www.cisco.com/go/prime>

Deployment Details

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

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

Commands at a CLI or script prompt:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000  
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

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

Installing and Configuring Cisco Prime Infrastructure

PROCESS

1. Obtain a license
2. Download trial software
3. Install software
4. Customize the VMware environment
5. Configure Prime Infrastructure
6. Apply software patches
7. Configure browser settings
8. Configure Prime Infrastructure basic settings
9. Configure user authentication
10. Configure users and user groups
11. Discover network devices
12. Configure software image management settings
13. Configure syslog host settings

Cisco Prime Infrastructure offers a single software installation that can manage up to 18,000 devices of various types.

Procedure 1 Obtain a license

If you are installing Cisco Prime Infrastructure for a unlicensed short-term trial only, skip this procedure and go to Procedure 2: Download trial software.

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.

When you purchase a product DVD, it comes with a Product Authorization Key (PAK). The PAK is normally printed on the software claim certificate included with product DVD kit.

Step 1: In a web browser, go www.cisco.com and log in.

Step 2: In the address box of the browser window, enter:

www.cisco.com/go/license

Step 3: Follow the product license registration instructions and use the PAK that you were given.

Procedure 2 Download trial software

Use this procedure to order a short-term trial copy of Cisco Prime Infrastructure.

If you already have Cisco Prime Infrastructure software, skip this procedure and continue with Procedure 3: Install software.

Step 1: In a web browser, go to www.cisco.com and log in.

Step 2: After you log in, go to the following site:

<http://cisco.com/go/nmsevals>

Step 3: On the left, under Cisco Prime Trial Downloads, click **All Items**, click Cisco Prime Infrastructure 2.1 (Express), and then follow the instructions in the browser to complete the order.

The screenshot shows the Cisco Store interface. The top navigation bar includes links for Solutions, Products & Services, Ordering, Support, Training & Events, and Partner Central. The main content area is titled 'Cisco Prime Infrastructure 2.1 (Express)'. It features a 'Product Description' section with text about the solution's capabilities and a 'Free Download' dropdown menu. The sidebar on the left lists various software categories, including 'Cisco Prime Trial Downloads' and 'Cisco Prime Not-For-Resale'.

After you complete the trial software order, you are sent an order confirmation email at the address associated with your cisco.com profile.

Step 4: Click **Download** to download and save the software.

Procedure 3 Install software

You install the Cisco Prime Infrastructure virtual appliance by using the Prime Infrastructure Open Virtualization Archive (OVA) image.

Before installing, make sure that your system meets the recommended hardware and software specifications listed in the Cisco Prime Infrastructure release notes.

- The duration of the software installation process varies for local-system installation versus virtual-environment installation:
 - Local-system installation—Approximately one-half hour
 - Virtual-environment installation—Approximately one hour
- Soft appliance OVA software can be installed only in a VMware environment.



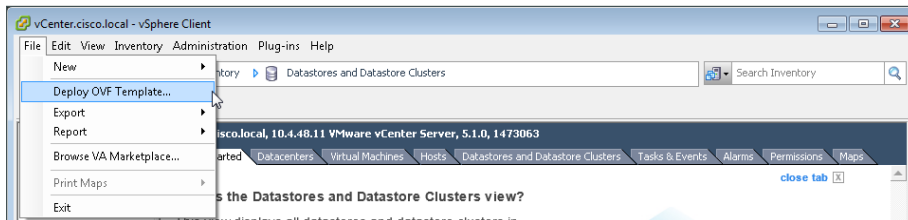
Tech Tip

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

Before installing the Cisco Prime Infrastructure soft appliance:

- Configure DNS entries for each network device.
- Enable Simple Network Management Protocol (SNMP), Secure Shell (SSH) Protocol, and Secure Copy Protocol (SCP) on the devices you are going to manage.
- Create an email address on your internal email server that Cisco Prime Infrastructure will use in order to send reports to subscribed users.

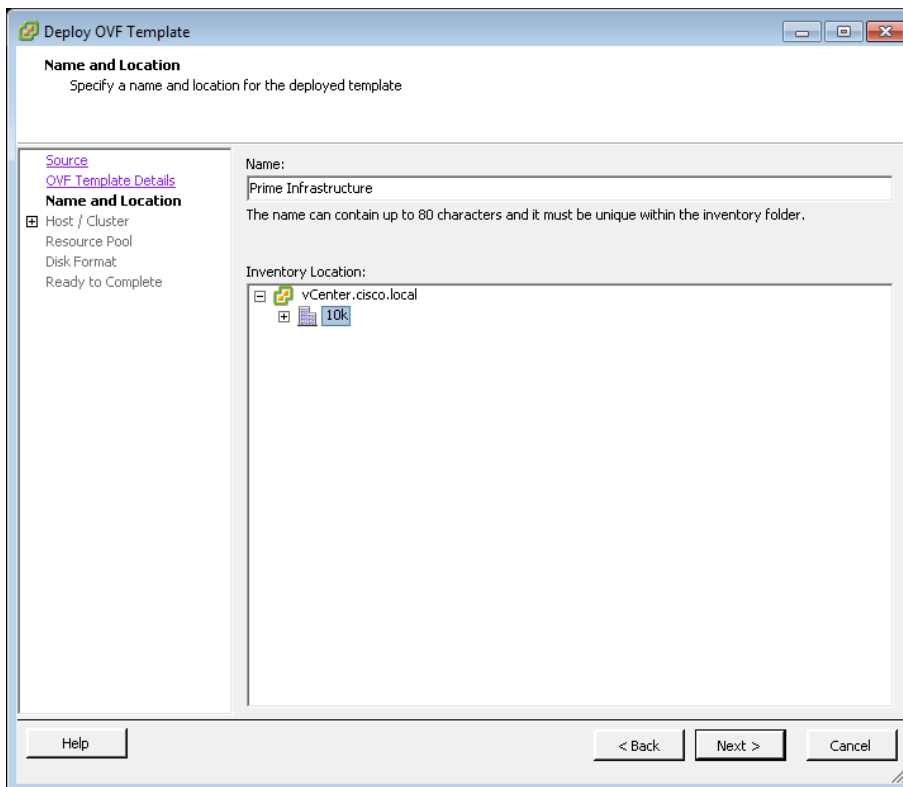
Step 1: In the VMware vSphere client, click **File** and then choose **Deploy OVF Template**.



Step 2: In the Deploy OVF Template wizard, on the Source page, browse to the location of the Cisco Prime Infrastructure OVA file and then click **Next**.

Step 3: On the OVF Template Details page, review the OVF template details and then click **Next**.

Step 4: On the Name and Location page, enter a unique and descriptive name for the virtual appliance that you are installing (Example: Prime Infrastructure), choose a location to install the virtual appliance, and then click **Next**.

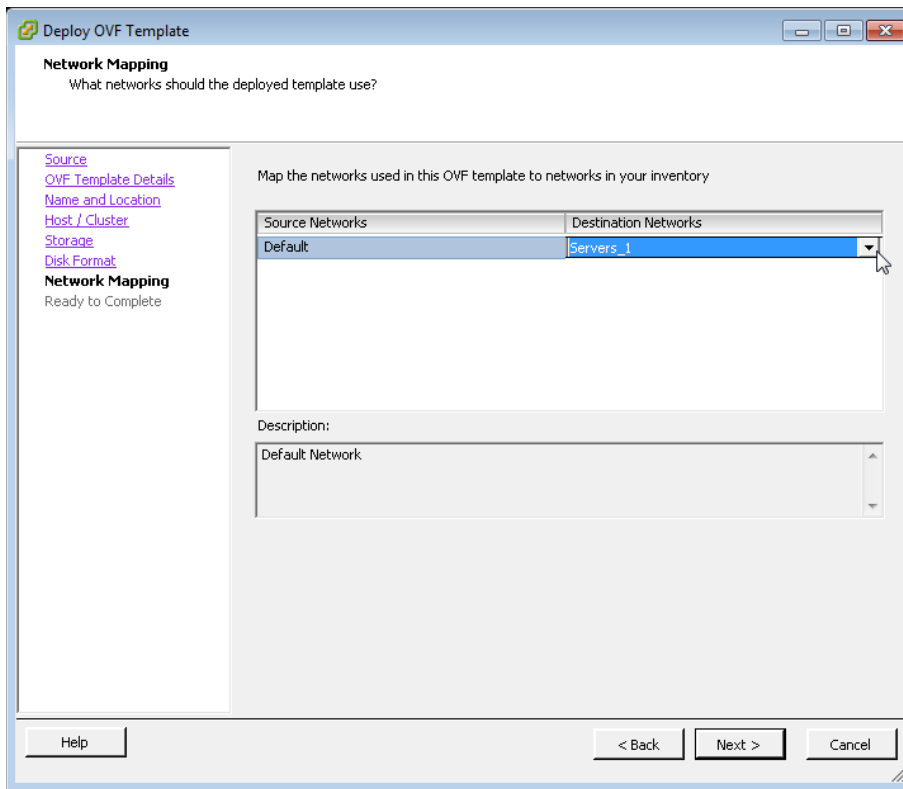


Step 5: On the Host/Cluster page, choose the host or cluster on which to install this virtual machine and then click **Next**.

Step 6: On the Storage page, choose where you want to store the virtual machine files and then click **Next**.

Step 7: On the Disk Format page, select **Thick Provision Lazy Zeroed** and then click **Next**.

Step 8: On the Network Mapping page, in the Destination Networks column, choose the appropriate network mapping group previously defined to the VMware environment (Example: Servers_1), and then click **Next**.



Step 9: On the Ready to Complete page, review the selected options, and then click **Finish**. The OVF installation of Cisco Prime Infrastructure begins.

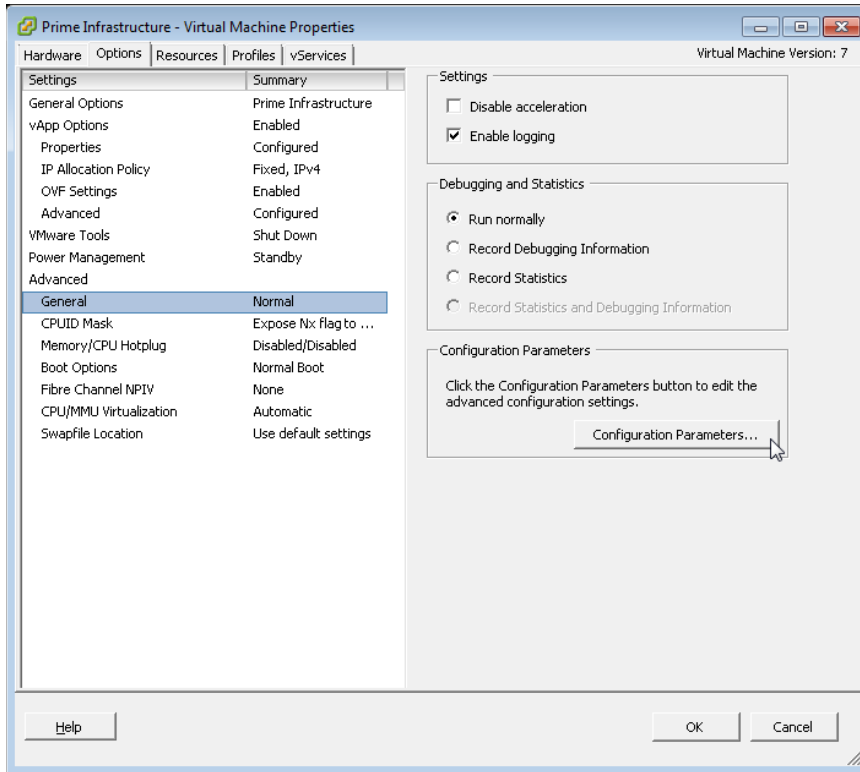
Procedure 4 Customize the VMware environment

(Optional)

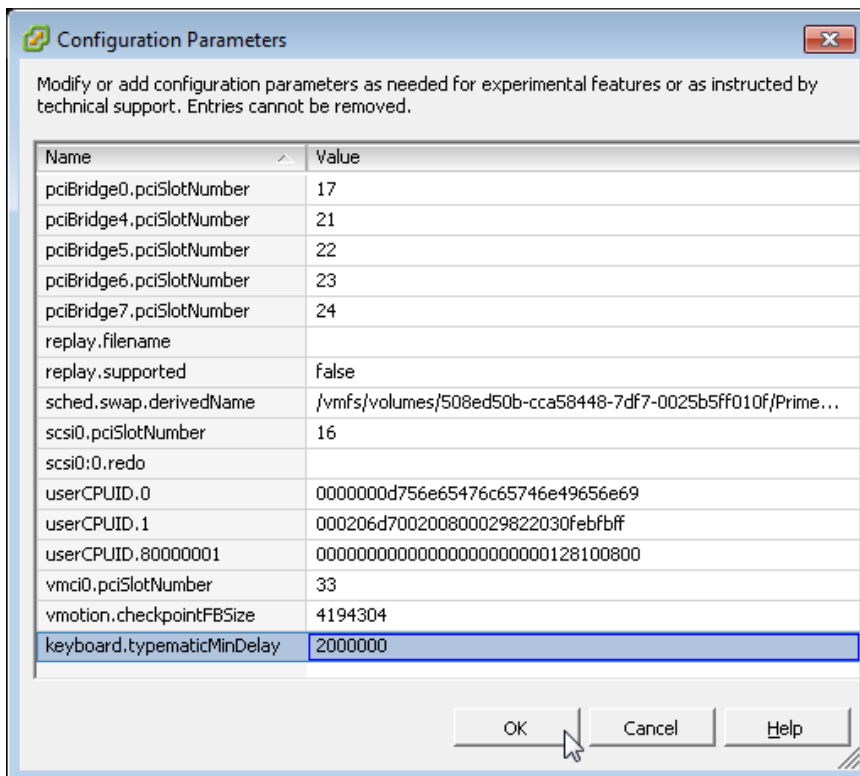
If you find that key strokes are repeating when entering various settings, it may be necessary to configure a keyboard delay value. This procedure is optional but is included here in the event that it is required.

Step 1: Using the VMware vSphere client, access the VMware vCenter environment, while the virtual machine is not in Power On state, highlight the Prime Infrastructure virtual host just installed, and then on the Getting Started tab, click **Edit virtual machine settings**.

Step 2: On the Virtual Machine Properties dialog box, click the **Options** tab, under Advanced, select **General**, and then click **Configuration Parameters**.



Step 3: On the Configuration Parameters dialog box, click **Add Row**, in the Name column, enter **keyboard.typematicMinDelay**, and in the Value column, enter **2000000** (2 million), and then click **OK**.



Step 4: On the Virtual Machine Properties dialog box, click **OK**.

Step 5: On the newly installed virtual machine, click the **Getting Started** tab, and then click **Power on the virtual machine**.

Procedure 5 Configure Prime Infrastructure

Step 1: Access the **Console** tab, and at the localhost login prompt, enter **setup**. This one-time login automatically starts the setup script.

```
*****  
Please type 'setup' to configure the appliance  
*****  
localhost login: setup
```

Step 2: In the startup script, enter the following configuration details for the server :

- Hostname—**Prime-Infra**
- IP address—**10.4.48.35**
- IP netmask—**255.255.255.0**
- Default gateway—**10.4.48.1**
- DNS domain name—**cisco.local**
- Primary name server—**10.4.48.10**
- Add/Edit another name server? Y/N—**N**
- Primary NTP server—**10.4.48.17**
- Add/Edit secondary NTP server? Y/N—**N**
- System time zone—**PST8PDT**
- Change system clock time? Y/N—**N**

Step 3: When prompted, create a username and password for accessing the Cisco Prime Infrastructure appliance console. This user will have the privilege to enable the shell access.

The default username is **admin**. You can use only alphanumeric characters for the username.

The password must have one upper case character (Example: C1sco123). By default, this password is set as the shell password.



Tech Tip

You cannot use **root** as the username because it is a reserved username.

Step 4: If you are planning to use this server as a standalone server or if this is the first or primary server, at the **Will this server be used as a Secondary for HA?** prompt, enter **no**.

Step 5: Enter and confirm the password for the root account that will be used to access the GUI through a browser. This password cannot be a variation of the word Cisco, and must contain a minimum of five characters. It is also used for the System Identity account. (Example: 1Qazxsw2)

Step 6: Enter and confirm an FTP password (Example: 1Qazxsw2), review the settings, and then at the **Apply these settings?** prompt, enter Y.

It takes 15 to 20 minutes to process the database engine, and then the server automatically reboots.

After the reboot, it takes some time before the system initializes and is ready for operation. When the server is ready, a login prompt is displayed.

```
Prime-Infra login:
```

Procedure 6 Apply software patches

If you intend to apply any recommended software patches to Cisco Prime Infrastructure, you should do that now. If you do not intend to apply any patches, skip to the next procedure.

Step 1: Establish an FTP server on the network and ensure that it has IP reachability to the VM running Cisco Prime Infrastructure. The FTP server must have the software patch accessible for the FTP user account that you use to access the repository.

Step 2: Use an SSH client to access the CLI of the Cisco Prime installation. Login using the admin username and password created during the initial installation. (Example: admin/C1sco123)

Step 3: Enter configuration mode.

```
Prime-Infra/admin# configure terminal  
Enter configuration commands, one per line. End  
with CNTL/Z.
```

Step 4: Create the software repository.

```
Prime-Infra/admin(config)# repository My-Prime-Repository
```

Step 5: Assign the remote repository a URL by entering `url ftp://[FTP server IP address]`.

```
Prime-Infra/admin(config-Repository)# url ftp://10.4.48.250
```

Step 6: Assign the remote repository username and password. This is the username and password for the FTP server.

```
Prime-Infra/admin(config-Repository)# user root password plain C1sco123  
<CTRL + Z>
```

Step 7: Enter `show repository [Repository Name]` and verify that the patch filename is displayed.

```
Prime-Infra/admin# show repository My-Prime-Repository  
PI_2.1_W_Y_Update_Y-Z.gz  
Prime-Infra/admin#
```

Step 8: Start the installation of the patch update by entering `patch install [Patch File Name] [Repository Name]`.

```
Prime-Infra/admin# patch install PI_2.1_W_X_Update_Y-Z.gz My-Prime-Repository
```


Step 9: When prompted to save the running configuration, confirm by pressing **Enter**.

```
Save the current ADE-OS running configuration? (yes/no) [yes] ?yes
```

The installation starts.

```
Generating configuration...  
Saved the ADE-OS running configuration to startup successfully  
Initiating Application Patch installation...
```

When installation completes successfully, the following message appears:

```
Patch successfully installed
```

Step 10: Verify that the installation is complete by entering the **show version** command. The web interface does not show the full version number but instead only shows the base version number. The **show version** command is the only way to verify that the patch has been applied to the base installation.

```
Prime-Infra/admin# show version  
Cisco Application Deployment Engine OS Release: 2.0  
ADE-OS Build Version: 2.0.6.003-px-build  
ADE-OS System Architecture: x86_64  
  
Copyright (c) 2005-2010 by Cisco Systems, Inc.  
All rights reserved.  
Hostname: Prime-Infra  
  
Version information of installed applications  
-----  
Cisco Prime Infrastructure  
-----  
Version : 2.1.0.0.87  
Patch: Cisco Prime Infrastructure Version: Update-Y Z for version 2_1_X Y  
Prime-Infra/admin#
```



Tech Tip

If you can't access the web interface after upgrading, verify that the NCS services are running by entering **ncs status** from within the CLI of Cisco Prime Infrastructure. If the services are not running, enter the **ncs start** command.

Procedure 7 Configure browser settings

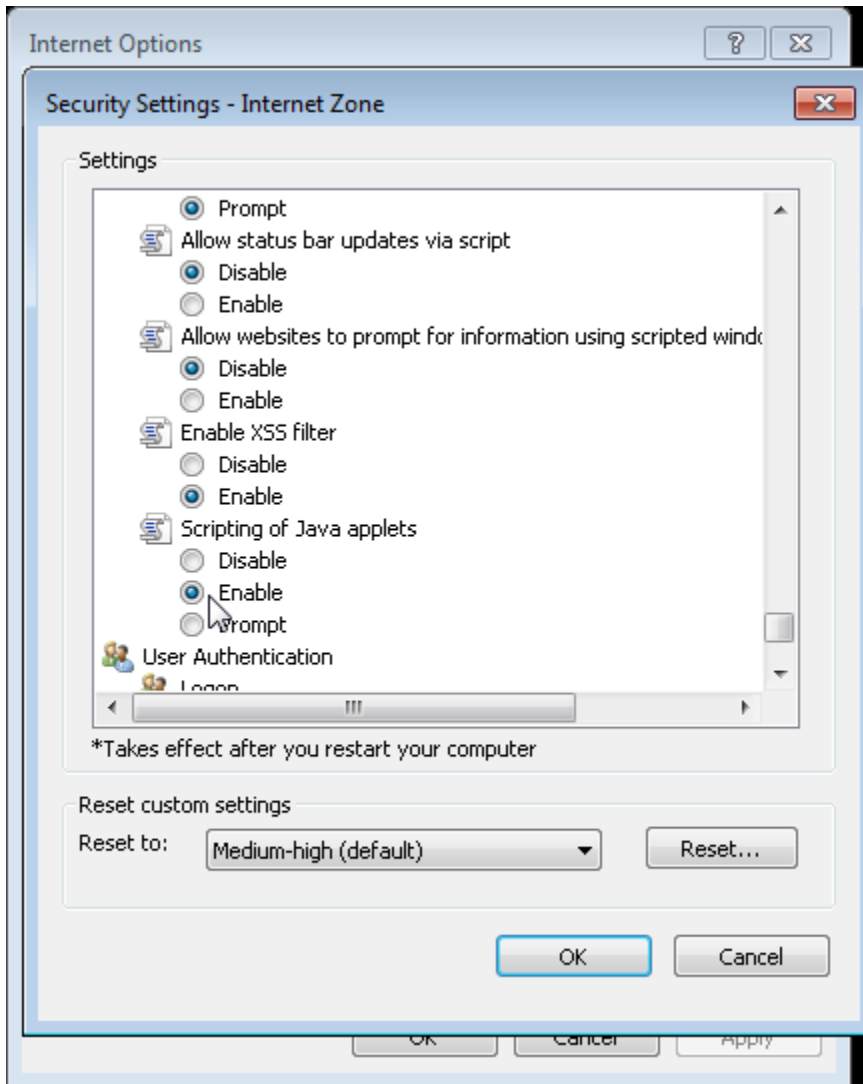
Cisco Prime Infrastructure supports specific web browser client configurations and versions. Management functionality can be impaired when you deviate from the supported clients. As an example, the supported versions of Internet Explorer require the Google Chrome Frame plugin. For the latest information about supported web browser clients, see the System Requirements references in the [Cisco Prime Infrastructure release notes](#).

Step 1: On the client machine, in a supported web browser, disable any pop-up blockers.

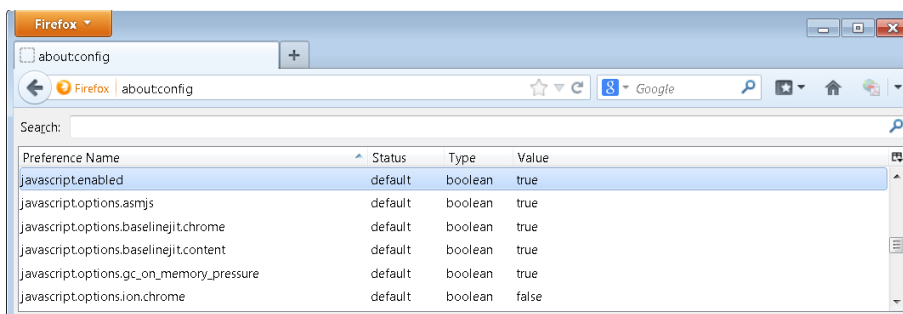
Some browsers allow you to enter the IP or hostname of specific sites that pop-up blocking should be disabled for. This approach allows pop-up blocking to be allowed globally with only those sites enter to be excluded.

Step 2: Enable JavaScript.

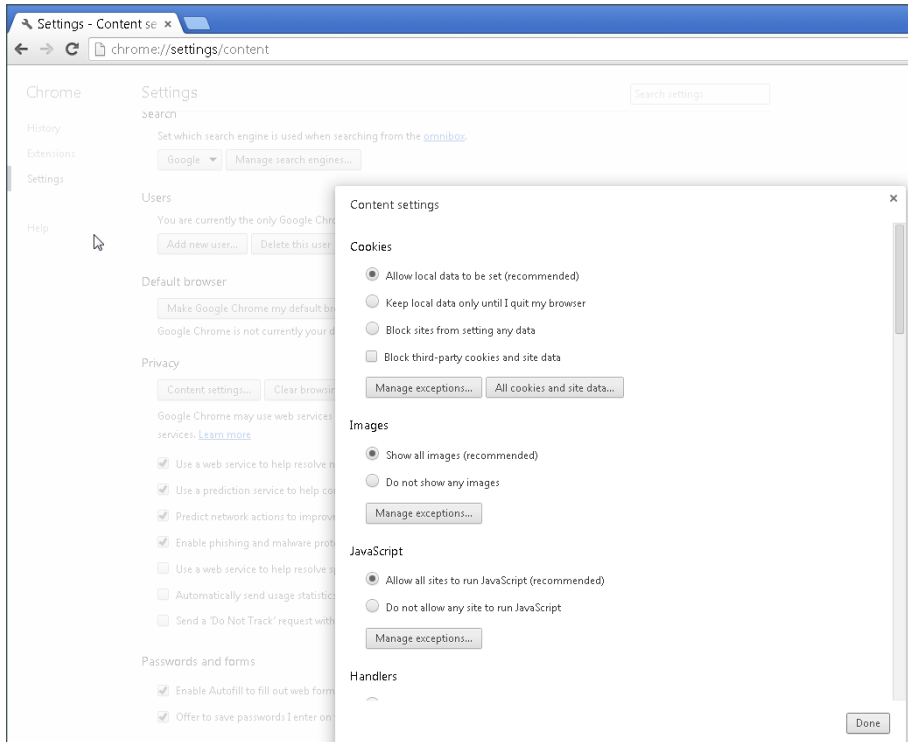
If you are using Internet Explorer 8 or later, navigate to **Tools > Internet Options > Security > Custom level > Settings**, and then under **Scripting > Scripting of Java applets**, select **Enable**.



If you are using Mozilla Firefox 25.0 or later, enter **about:config** in the navigation bar and accept the warning message. Find the **javascript.enabled** preference and ensure it is enabled. If it isn't, right-click it and choose **Toggle**.



If you are using Chrome 25.0 or later, enter **chrome://settings/content** in the navigation bar and verify that JavaScript is enabled.



Procedure 8 Configure Prime Infrastructure basic settings

Step 1: In a web browser, open the Cisco Prime Infrastructure web interface (Examples: <https://prime-infra.cisco.local> or <https://10.4.48.35>).

If you are installing in an evaluation environment without a registered certificate server, accept the certificate warnings.

If you receive a message about needing a more recent version of Adobe Flash Player, follow the installation instructions.

If you are using an unsupported web browser client, you may see a warning message as shown in the following figure. If you see this message, please return to the previous procedure for information about supported web browser clients.



Step 2: Log in by using the username **root** and the password that you provided during installation (Example: root/1Qazxsw2).



Step 3: Navigate to **Administration > System Settings**, click **Mail Server Configuration**.

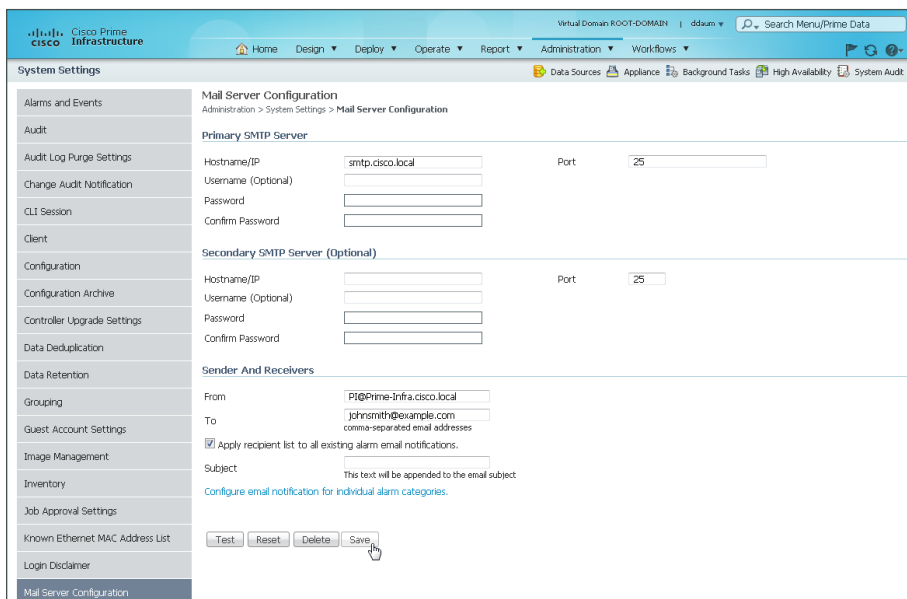
Step 4: Under Primary SMTP Server, in the **Hostname/IP** box, enter the host name of the SMTP server (Example: smtp.cisco.local).

Step 5: Under Senders And Receivers, in the **From** box, enter the email address from which you want to send notifications.

Step 6: In the **To** box, enter the email address to which you want notifications sent.

Step 7: Select **Apply recipient list to all existing alarm email notifications**, and then click **Save**.

This enables you to receive email alerts about network issues, job status, report generation, etc.



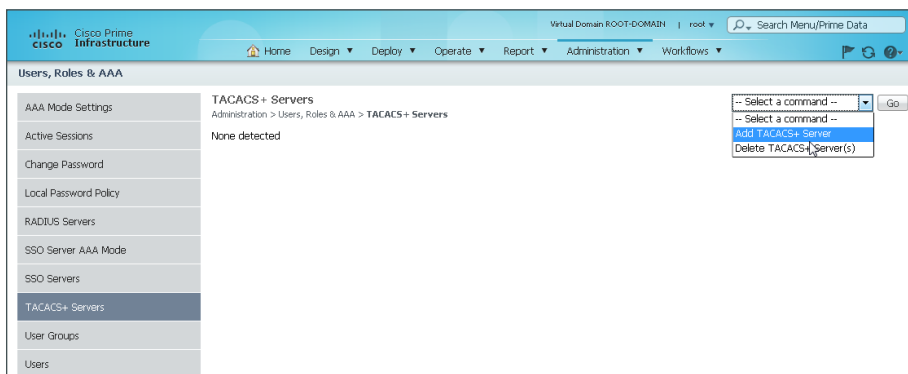
Procedure 9 Configure user authentication

(Optional)

Cisco Prime Infrastructure can use its local database, RADIUS, or TACACS+ in order 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 Cisco Prime Infrastructure to use TACACS+ authentication.

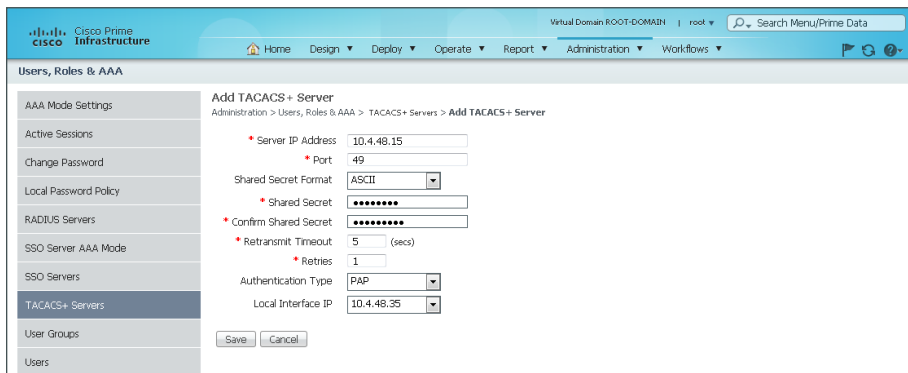
Step 1: Navigate to **Administration > Users, Roles & AAA**, and then in the left column, click **TACACS+ Servers**. The TACACS+ page appears.

Step 2: In the **Select a command** list in the upper right corner of the web page, choose **Add TACACS+ Server**, and then click **Go**.



Step 3: In the **Server IP Address** box, enter the IP address of the TACACS+ server (Example: 10.4.48.15)

Step 4: In the **Shared Secret** and **Confirm Shared Secret** boxes, enter the TACACS+ secret key (Example: SecretKey), and then click **Save**.



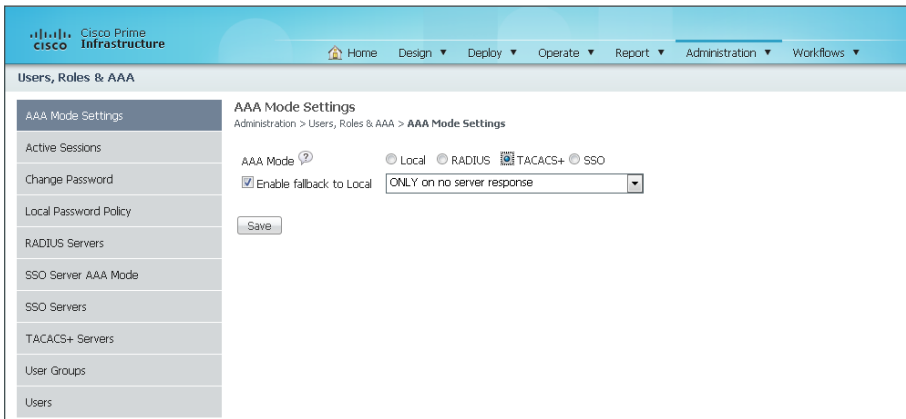
Step 5: Navigate to **Administration > Users, Roles & AAA**, and then in the left column click **AAA Mode Settings**.

The AAA Mode Settings page appears.

Step 6: Select **TACACS+**.

Step 7: Select the **Enable fallback to Local** option and then in the list, choose **ONLY on no server response**.

Step 8: Click **Save**.



Procedure 10 Configure users and user groups

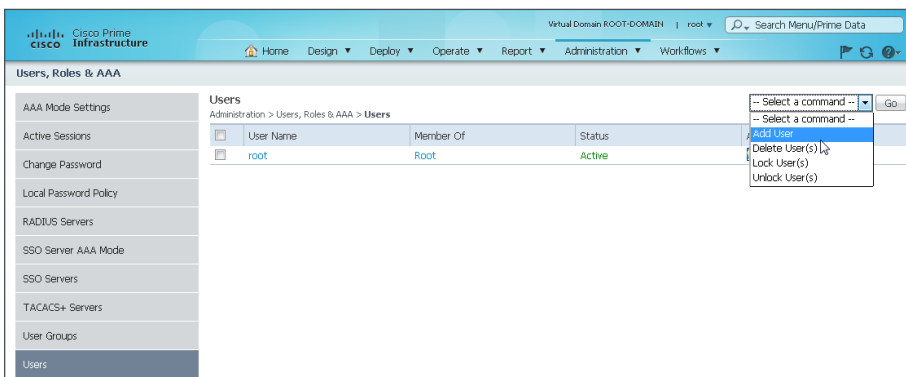
User groups (or roles) are collections of privileges that dictate the type of system access the user has. Some predefined roles are:

- **System Monitoring**—Users can access network status information only. They cannot perform any action on a device or schedule a job on a network.
- **Config Managers**—Users can perform all system monitoring tasks and tasks related to network data collection. They cannot perform any task that requires write access on the network.
- **Admin**—Users can monitor and configure operations and perform all system administration tasks.
- **Super Users**—Users can perform all Cisco Prime Infrastructure operations, including administration and approval tasks.

When using an authentication module other than the Cisco Prime Infrastructure local database, Prime Infrastructure authenticates the user against the external module. After the user is successfully authenticated, Prime Infrastructure assigns the configured role to this user.

Step 1: Navigate to **Administration > Users, Roles & AAA**, and then in the left column click **Users**.

Step 2: In the **Select a command** list, choose **Add User**, and then click **Go**.



The Add Users screen appears, with the General tab selected.

Step 3: Enter the username and password.

Step 4: Under Groups Assigned to this User, select the role for the user, and then click **Save**.

The screenshot shows the Cisco Prime Infrastructure web interface. The main content area is titled 'Add User' and is part of the 'Users, Roles & AAA' configuration. The 'General' tab is selected. The 'Username' field contains 'ExampleAdministrator'. The 'New Password' and 'Confirm Password' fields are masked with dots. Below these fields is a section titled 'Groups Assigned to this User' with a list of roles and checkboxes: Admin, Config Managers, Lobby Ambassador, Monitor Lite, NBI Credential, North Bound API, Root, Super Users (checked), and System Monitoring. At the bottom of the form are 'Save' and 'Cancel' buttons. A mouse cursor is pointing at the 'Save' button.

Step 5: For each user you need to create, repeat this procedure.

Procedure 11 Discover network devices

Before Cisco Prime Infrastructure can manage a device, the device must be in the database. You can add devices to the database in three ways:

- Discover the devices by using a discovery protocol
- Add devices manually
- Import devices in bulk

Cisco Prime Infrastructure supports Layer 2 and Layer 3 protocols for device discovery. Cisco Discovery Protocol (CDP) is the preferred protocol for discovering network devices.

Before you perform this procedure, you must enable both CDP and SNMP on all devices that you want to manage. If you did not deploy your network by using the [Campus Wireless LAN Technology Design Guide](#), which enables both of these protocols, see the Cisco Prime Infrastructure production documentation for guidance:

<http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/index.html>

This procedure uses a number of Cisco Prime Infrastructure Discovery features—including Layer-2-based CDP, SNMP v2, and SSH.

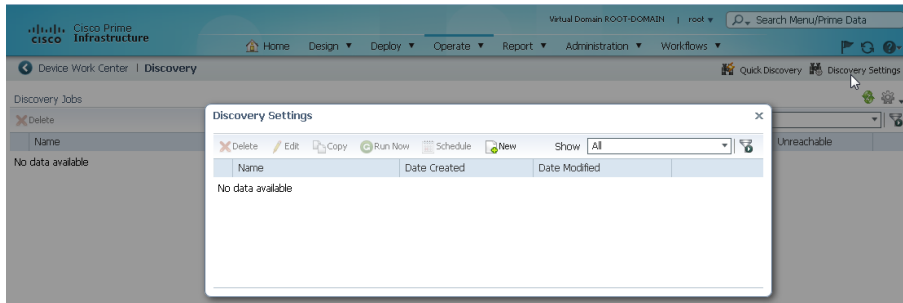
i Tech Tip

Before discovering devices, it is recommended that you check for the latest Cisco Prime Infrastructure Device Package Update and read the release notes in order to understand if the software update is appropriate for your deployment. You can look for the latest Device Package Update by navigating to **Administration > Software Update**, and then clicking on **Upload Update File** to get instructions for downloading and installing the updates from your web browser. When the update is available within Cisco Prime Infrastructure, you can use the Software Update interface to easily observe the support information associated with the updates.

Step 1: Navigate to **Operate > Device Work Center > Discovery**.

Step 2: In the upper right corner, click **Discovery Settings**.

The Discovery Settings dialog box appears.



Step 3: Click **New**.

A second, blank Discovery Settings dialog box appears. In the following steps, the values that you enter are the default credentials that Cisco Prime Infrastructure uses when it connects to discovered devices when it performs jobs for device inventory, configuration archive, and software image management.

Discovery Settings

*Name

Current Discovery Settings

Protocol Settings

PingSweep Module ?

▶ **Layer 2 Protocols**

▶ **Advanced Protocols**

Filters ?

IP Filter ?

▶ **Advanced Filters**

Credential Settings

SNMPv2 Credential ?

SNMPv3 Credential ?

Telnet Credential ?

SSH Credential ?

Preferred Management IP ?

Use Loopback

Step 4: In the **Name** box, enter **My_Discovery_Settings**.

Step 5: Expand **Layer 2 Protocols**, and then next to **CDP Module**, click the **+** icon.

Step 6: In the expanded **CDP Module** area, select **Enable Cisco Discovery Protocol** and select **Enable Cross Router Boundary**.

Step 7: Click **Add Row**. If your browser collapses the view, click the **+** icon again to expand it.

Step 8: In the **Seed Device** box, enter the management IP address for the core switch (Example: 10.4.40.254) and a Hop Count (Example: 11), and then below the Seed Device box, click **Save**.

i Tech Tip

The neighbor devices from the CDP-MIB are gleaned and then also queried for neighbors, and then the discovery process repeats. Depending on the network, this could be a large number of devices. In large networks, it is recommended that you restrict the scope of the discovery by adding an appropriate Hop Count value.

| Seed Device | Hop Count |
|-------------|-----------|
| 10.4.40.254 | 11 |

Step 9: Under Credential Settings, next to SnmpV2 Credential, click the + icon.

Step 10: In the expanded SnmpV2 Credential area, select **Enable SnmpV2 Credential**.

Step 11: Click **Add Row**.

Step 12: Enter an IP address, using an asterisk wildcard to represent an octet. For example, if all devices on your network use the same community string, enter: *.*.*

Step 13: Enter the read and write community strings (Examples: cisco, cisco123).

Step 14: Below the IP box, click **Save**.

| IP | Read Community String | Write Community String | SNMP Tim... |
|------|-----------------------|------------------------|-------------|
| **** | ***** | ***** | 3 |

Tech Tip

Adding the read/write community string is critical for wireless management because Cisco Prime Infrastructure will add the MSE-VA Key Hash and MAC address value to each of the synchronized wireless LAN controllers using SNMP SET commands. The use of the Read/Write community string is therefore required.

Step 15: Next to SSH Credential, click the + icon.

Step 16: Select **Enable SSH Credential**.

Step 17: Click **Add Row**.

Step 18: Enter an IP address, using an asterisk wildcard to represent an octet. For example, if all devices on your network use the same SSH credentials, enter: ****

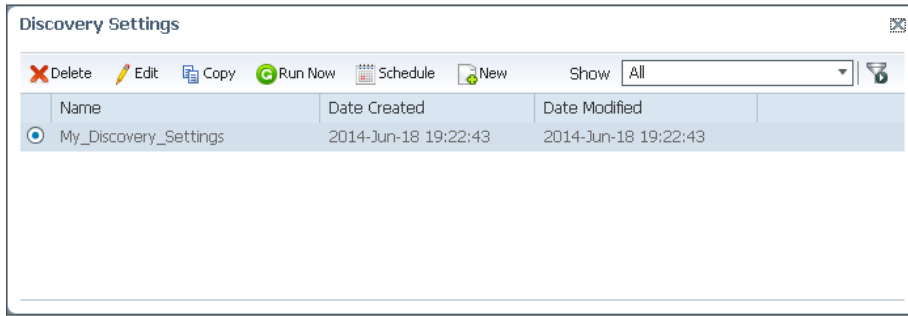
Step 19: Enter the username, password, and enable password.

Step 20: Select **SSHv2**, and then below the User Name box, click **Save**.

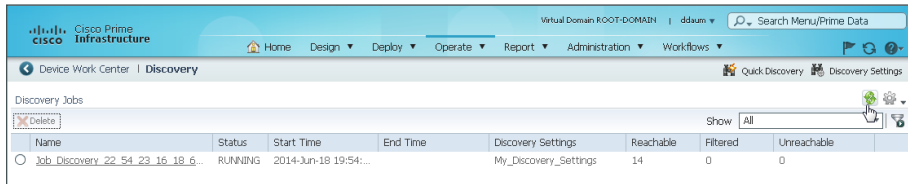
| IP | User Name | Password | Enable Passw... |
|------|-----------|----------|-----------------|
| **** | ***** | ***** | ***** |

Step 21: Click Run Now.

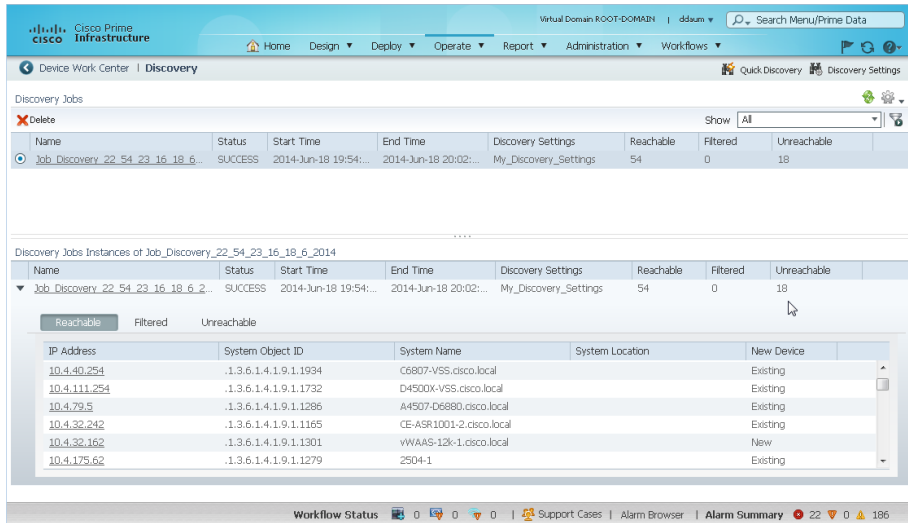
The discovery settings are saved and Cisco Prime Infrastructure begins device discovery. The amount of time this discovery process takes depends on the number of devices on the network.



Step 22: If you want to view the discovery progress, click **Operate > Discovery**. If you want to instantly update the in-progress results, click the green refresh icon in the upper right corner.



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



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

Procedure 12 Configure software image management settings

The network deployment described in the [Campus Wired LAN Technology Design Guide](#) does not enable Telnet or TFTP on Cisco network devices. This procedure describes how to enable Cisco Prime Infrastructure to distribute software images to devices using Secure Copy Protocol (SCP).

Tech Tip

To distribute images by SCP, you may need to enable the SCP server feature on Cisco IOS devices. To do so, add the `ip scp server enable` command to the running configuration. For examples of enabling the SCP server feature for network management of a device, see the [Campus Wired LAN Technology Design Guide](#).

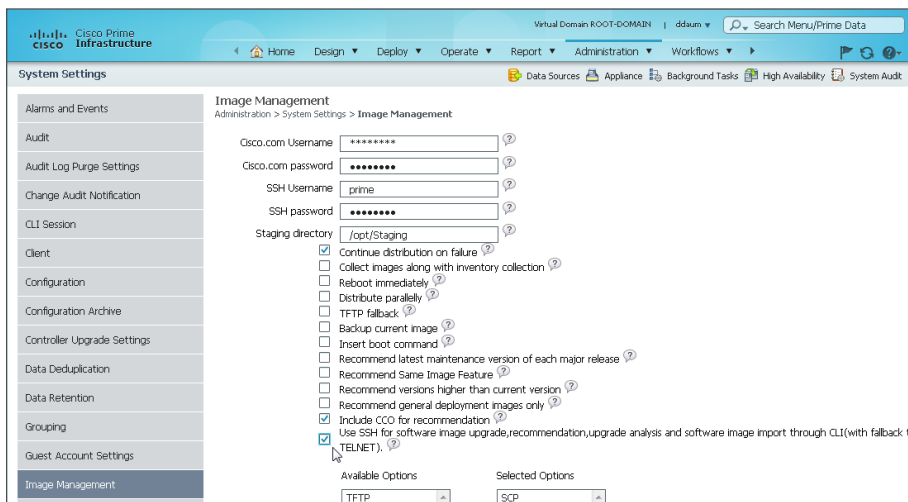
Step 1: Navigate to **Administration > System Settings** and then in the left column click **Image Management**.

Step 2: In the **Cisco.com user name** and **Cisco.com password** boxes, enter the credentials for a Cisco.com account that has permissions to download software.

Step 3: Enter the **SSH Username** and **SSH password** for a user that has access to manage the devices.

Step 4: Ensure that **TFTP fallback** is not selected.

Step 5: Select **Use SSH for software image upgrade, recommendation, upgrade analysis and software image import through CLI (with fallback to TELNET)**.



Virtual Domain: ROOT-DOMAIN | ddsun | Search Menu/Prime Data

System Settings

Image Management
Administration > System Settings > Image Management

Cisco.com Username: *****

Cisco.com password: *****

SSH Username: prime

SSH password: *****

Staging directory: /opt/Staging

- Continue distribution on failure
- Collect images along with inventory collection
- Reboot immediately
- Distribute parallelly
- TFTP fallback
- Backup current image
- Insert boot command
- Recommend latest maintenance version of each major release
- Recommend Same Image Feature
- Recommend versions higher than current version
- Recommend general deployment images only
- Include CCO for recommendation
- Use SSH for software image upgrade, recommendation, upgrade analysis and software image import through CLI (with fallback to TELNET)

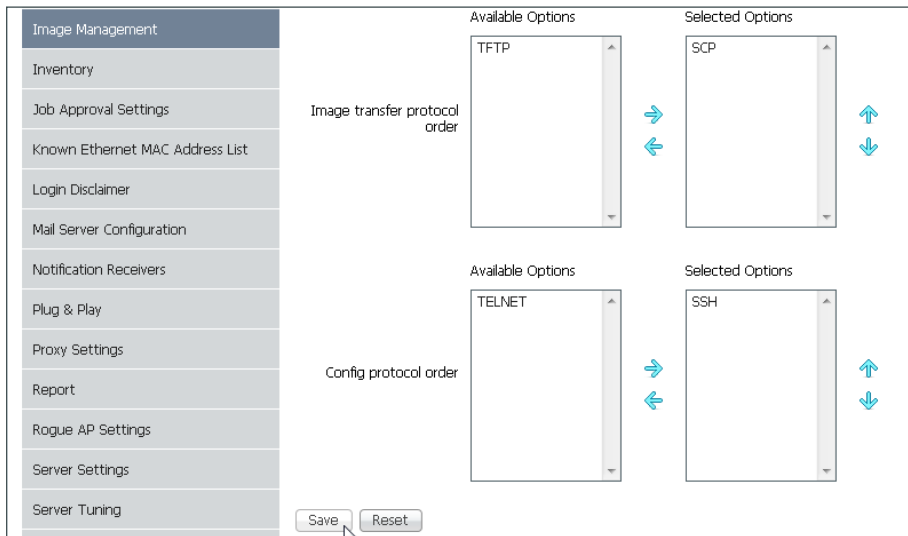
Available Options: TFTP

Selected Options: SCP

Step 6: In the **Image transfer protocol order** dual list, ensure that **SCP** is in the right list. Protocols in the right list are used by Prime Infrastructure. Also, ensure that **TFTP** is in the left list, which shows the protocols that are not used.

Step 7: In the **Config protocol order** dual list, ensure that **SSH** is in the right list. Also, ensure that **TELNET** is in the left list, which shows the protocols that are not used.

Step 8: Click Save.



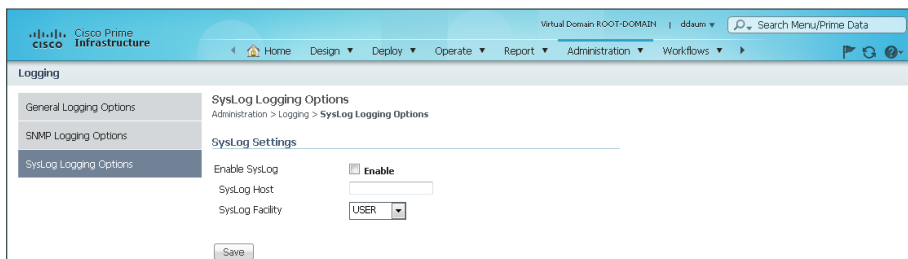
Procedure 13 Configure syslog host settings

Cisco Prime Infrastructure can act as a logging host for system messages sent by managed devices.

Tech Tip

Managed devices must be configured to send system messages to Cisco Prime Infrastructure. After devices are successfully discovered by Prime Infrastructure, you can use the CLI template to configure logging on devices. For an example of using the logging configuration template, see the Deploy CLI templates procedure.

Step 1: Navigate to **Administration > Logging** and then, in the left column, click **SysLog Logging Options**. The SysLog Logging Options page appears.

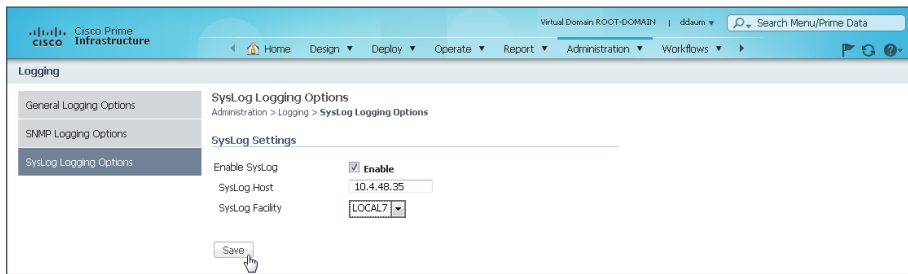


Step 2: Next to Enable Syslog, select **Enable**.

Step 3: In the **SysLog Host** box, enter **10.4.48.35**.

Step 4: In the **SysLog Facility** list, choose **LOCAL7**.

Step 5: Click **Save**.



Step 6: To see syslog messages from managed devices that are correctly configured to send system messages to Prime Infrastructure, navigate to **Operate > Alarms and Events** and then click the **Syslogs** tab.

PROCESS

Managing the Network

1. Import and distribute software images
2. Customize monitoring
3. Customize and schedule reports
4. Deploy CLI templates

Procedure 1 Import and distribute software images

The Software Image Management feature enables you to keep a library of Cisco software images and to distribute software images to managed devices. Cisco Prime Infrastructure enables you to upgrade a managed device to an image.

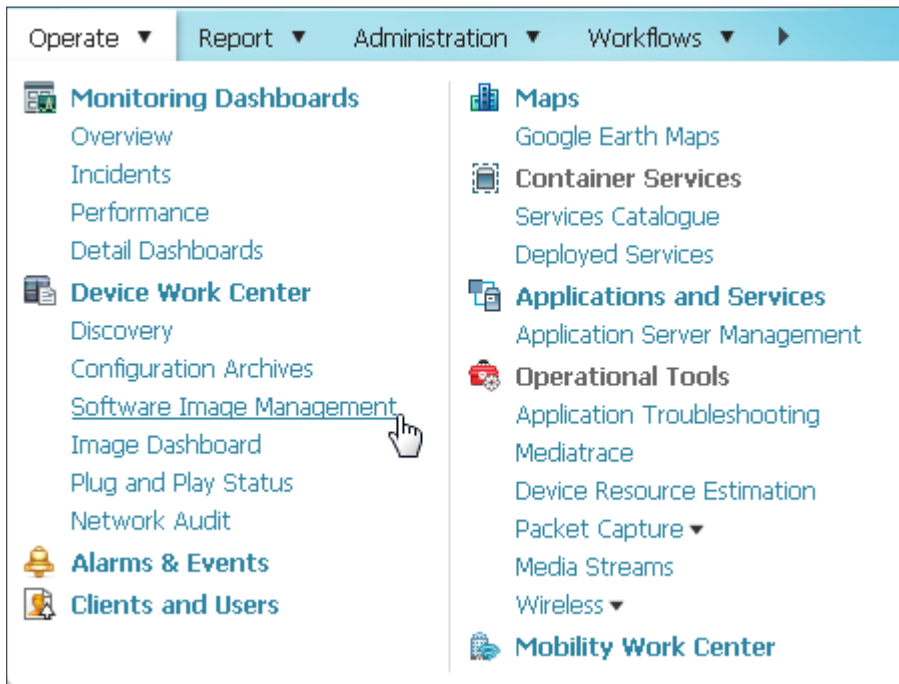
You can add to the repository software images that you import from Cisco.com, a managed device, a file system, or a URL.

i Tech Tip

To distribute images by SCP, you may need to enable the SCP server feature on Cisco IOS devices. To do so, add the **ip scp server enable** command to the running configuration. For examples of enabling the SCP server feature for network management of a device, see the [Campus Wired LAN Technology Design Guide](#).

To download a software image from cisco.com and distribute it to a device, perform this procedure.

Step 1: Navigate to **Operate > Device Work Center**, and then click **Software Image Management**.



Step 2: Click **Import**.

The Import Images dialog box appears. As you make selections and choices, the Import Images dialog box updates.

Step 3: Under **Source**, select **Cisco.com**.

Step 4: In the **Select Device Platform** list, choose the type of Cisco device for which you want a software image.

Step 5: In the **Select Image Version** list, choose the version of the software image.

Step 6: In the **Select Feature Package** list, choose the feature package for the software image.

Step 7: Under Schedule, configure the following items:

- **Job Name**—Enter a descriptive name for the Cisco.com software image import job.
- **Start Time**—Select **Now**.

Import Images

Source

Device

Cisco.com

URL

File

Collection Options

Select Device Platform: CAT6000-VS-S2T

Select Image Version: 15.1.2-SY2

Select Feature Package: CED IP SERVICES FULL ENCRYPT

Selected Image: s2t54-advipservices9-mz.SPA.151-2.SY2.bin

Schedule

Job Name: Job_CCO_Image_Collection_11_40_29_962_PM_18_5_2014

Start Time: Now Date: 06/18/2014 08:40 PM (MM/dd/yyyy hh:mm AM/PM)

Submit Cancel

Step 8: Click **Submit**.

Cisco Prime Infrastructure begins the software image import job.

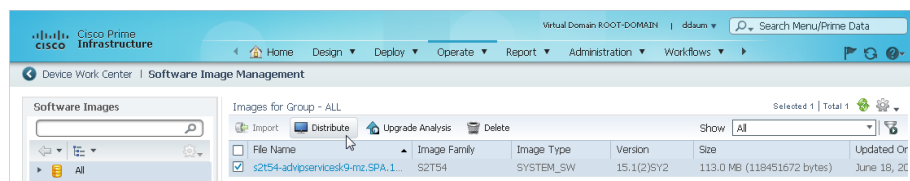
i Tech Tip

To view the status of the job, navigate to **Administration > Jobs Dashboard** and look for the job name that you entered.

If importing software from Cisco.com fails, go to www.cisco.com, login with the credentials that you provided in Procedure 12, and ensure that you can download software.

Step 9: After Cisco Prime Infrastructure has imported the software image, return to **Operate > Software Image Management**.

Step 10: Select the software image and click **Distribute**.



The Distribute Images dialog box lists the managed devices that are compatible with the selected software image.

Step 11: Under Device Selection, in the **Devices** list, select one or more devices to distribute the software image to.

Step 12: Under Distribute Image and Location Selection, verify the device and software image selected.

Step 13: Under Schedule Distribution, configure the following items:

- **Job Name**—Enter a descriptive name for the Cisco.com software image distribution job.
- **Start Time**—Select **Now**.

Distribute Images

▶ **Device Selection**

▶ **Distribute Image and Location Selection**

▶ **Distribution Options**

▼ **Schedule Distribution**

Job Name

Start Time **Now** **Date** (MM/dd/yyyy hh:mm AM/PM)

Step 14: Click **Submit**.

Cisco Prime Infrastructure begins the software image distribution job.

i **Tech Tip**

To view the status of the job, navigate to **Administration > Jobs Dashboard** and look for the job name that you entered.

Procedure 2 Customize monitoring

The role of monitoring in network management is so essential that the home page in the Cisco Prime Infrastructure web interface is the monitoring dashboard. This dashboard provides a unified view of all the activities being monitored by an administrator. Cisco Prime Infrastructure provides a comprehensive list of monitoring dashlets 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; and syslog information.

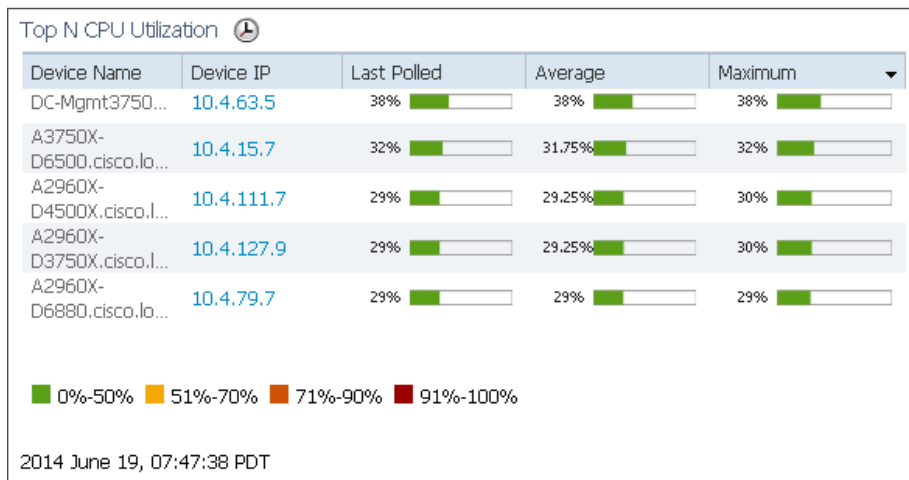
Each dashlet includes options that allow you to customize the dashlet to suit your needs. This procedure provides an example of how to customize the CPU utilization dashlet.

Step 1: Navigate to **Operate > Monitoring Dashboards > Performance**.

The monitoring page displays the performance monitoring dashboard.

Step 2: If the Network Device tab is not selected under Performance, click **Network Device**.

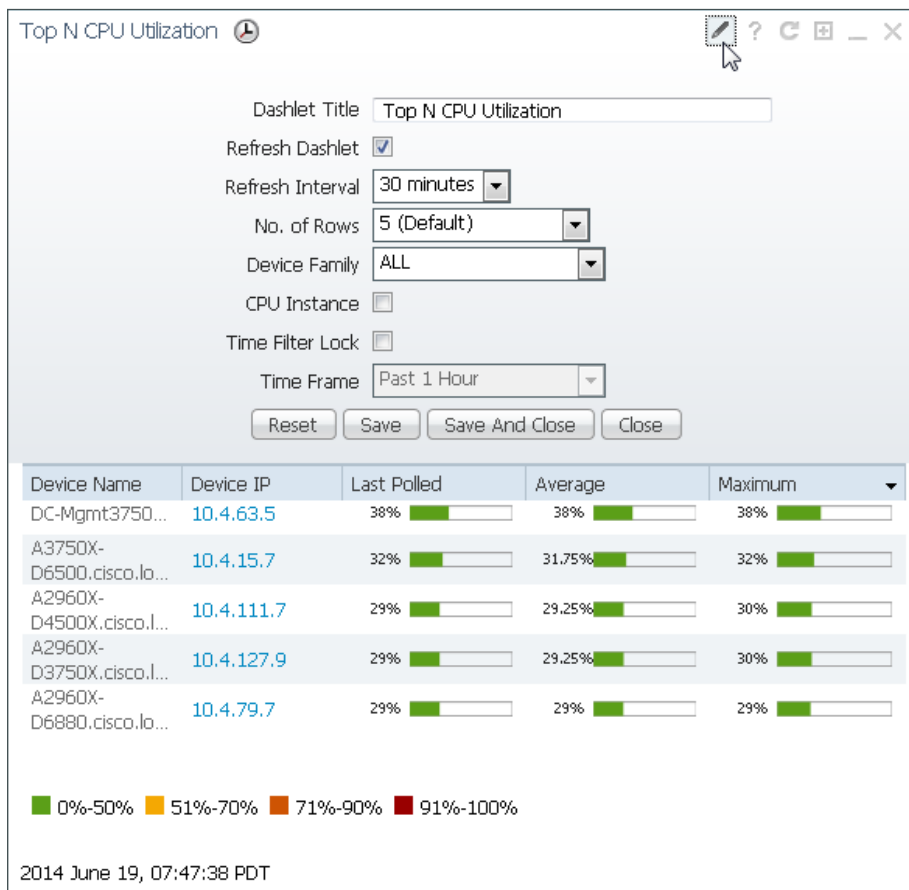
The Top N CPU Utilization dashlet appears, along with other network-device performance-monitoring dashlets. By default, you can view a list of devices with the top CPU utilization during the past hour.



Step 3: Move the mouse pointer to the upper right corner of the dashlet

The dashlet shows the Dashlet Options icon and icons for refreshing, maximizing, minimizing, and closing the dashlet.

Step 4: Click the Dashlet Options icon.



Step 5: Configure the options to suit your needs and then click **Save And Close**.

The dashlet shows the data in the way that you chose by configuring the options.

Procedure 3 Customize and schedule reports

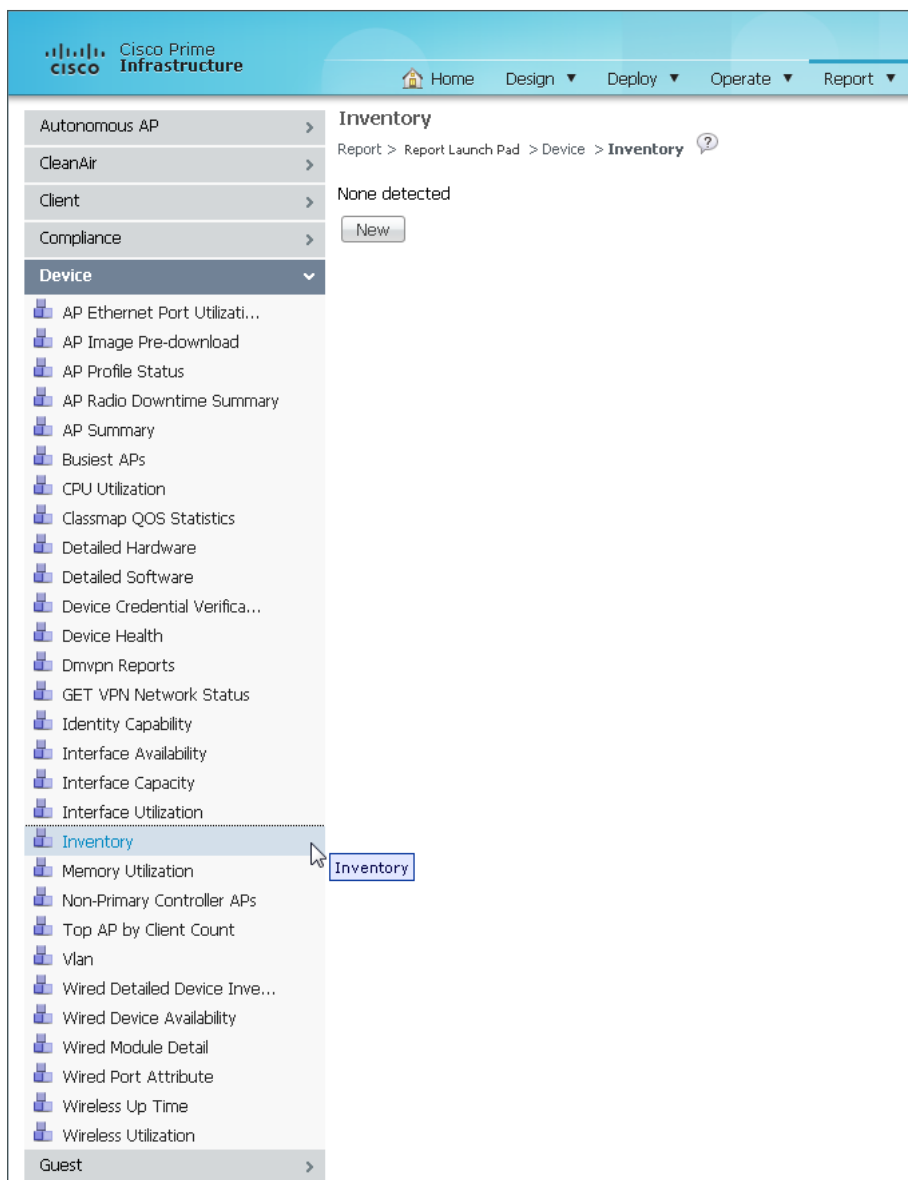
Prime Infrastructure provides you a single launch point for all reports that you can generate and view. The Report Launch Pad page provides access to over 100 reports, each of which you can customize as needed.

This procedure provides an example of how to customize and generate a device inventory report.

Step 1: Navigate to **Report > Report Launch Pad**.

The Report Launch Pad lists by category all available reports.

Step 2: On the left, click the **Device** category, and then click **Inventory**.



Step 3: Click **New**.

The Inventory : New page shows the report settings and schedule options.

Step 4: Under Settings, configure the following items:

- **Report Title**—Enter a descriptive report title (Example: Custom Switch Inventory).
- **Report Type**—Choose either a specific device type to be included in the report or **Combined Inventory** to include all managed devices in the report (Example: Switches).

The screenshot shows the Cisco Prime Infrastructure web interface. At the top, there is a navigation bar with the Cisco logo and 'Cisco Prime Infrastructure' text. Below the navigation bar, the page title is 'Inventory : New' and the breadcrumb trail is 'Report > Report Launch Pad > Device > Inventory > Inventory Report Details'. The main content area is titled 'Settings' and contains the following configuration options:

- Create reports in current and each sub Virtual Domains** (with a help icon and a link to 'View sub Virtual Domains')
- Report Title:
- Report Type:
- Customize Report: **Customize the data for this report**

Step 5: Click **Customize**.

Step 6: At the top in the Custom Report Name list, choose the subreport that includes the available fields that you want to see in your customized report (Example: Switch Inventory).

Step 7: If the report type has the option to contain tables, graphs, or both, you can select this by using the Report View list that appears below the Custom Report Name list.

Step 8: If you want to add or remove fields from the report, at and then use the Add and Remove buttons to configure the “Data fields to include” list.

Custom Report Name: Switch Inventory Do not include

Available data fields

- System Contact
- Last Boot Time
- Image Type
- Image Family
- Image Name

Data fields to include

- Device Name
- Description
- IP Address
- Location
- Reachability Status
- Software Version
- Product Type

* Blue fields are mandatory in this subreport.

Data field sorting

Sort by: None Ascending Descending

Then by: None Ascending Descending

Then by: None Ascending Descending

Then by: None Ascending Descending

* Only reports in tabular format can be sorted.
* Only fields that can be sorted appear in the selection menus.

After clicking Apply, click Save on the Report Details page to save the custom report settings.

Apply Reset Cancel

Step 9: Click **Apply**.

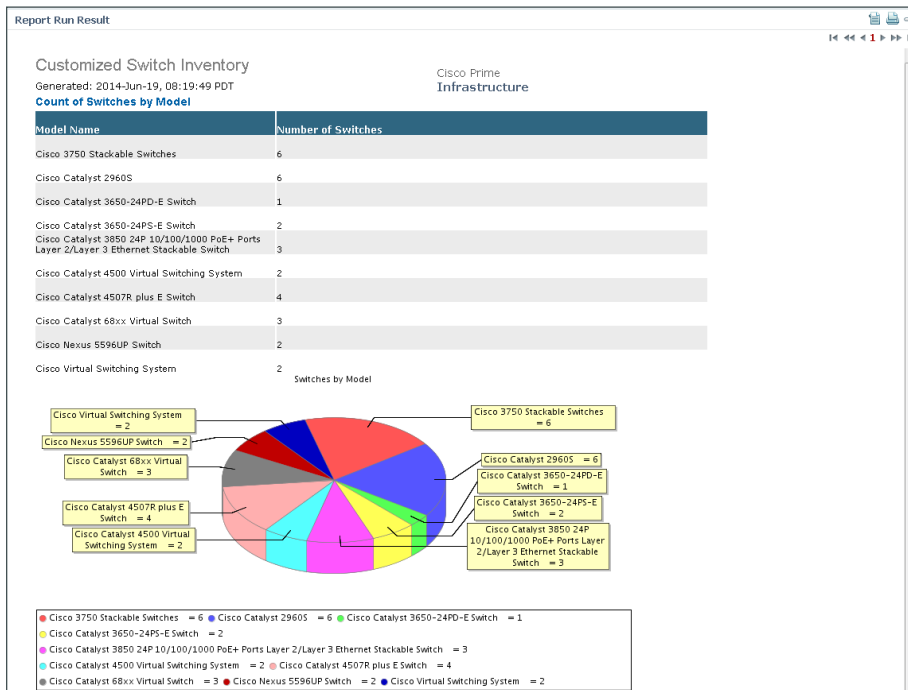
Step 10: If you want the report to run at a specific time, under **Schedule**, enter the following values:

- Scheduling Enable—**Selected**
- Start Date/Time—Specify the date and time for the report.

Step 11: If you want to run the report on a regular basis, select the recurrence basis—hourly, daily, weekly, or monthly—and specify the period.

Step 12: Click **Run and Save**.

When the report is complete, the Report Run Result area shows the report contents.



Tech Tip

If you want to access a list of reports that you have configured and saved, navigate to **Report > Saved Report Templates**.

Procedure 4

Deploy CLI templates

The Configuration Templates feature enables you to deploy device configuration commands to many devices with a single deployment job, including support for device-specific values.

Cisco Prime Infrastructure provides a set of command-line interface (CLI) templates. You can customize these templates to accommodate your needs or create your own templates. The CLI templates feature uses Apache Velocity Template Language (VTL). For more information about Apache VTL, see:

<http://velocity.apache.org/engine/devel/vtl-reference-guide.html>

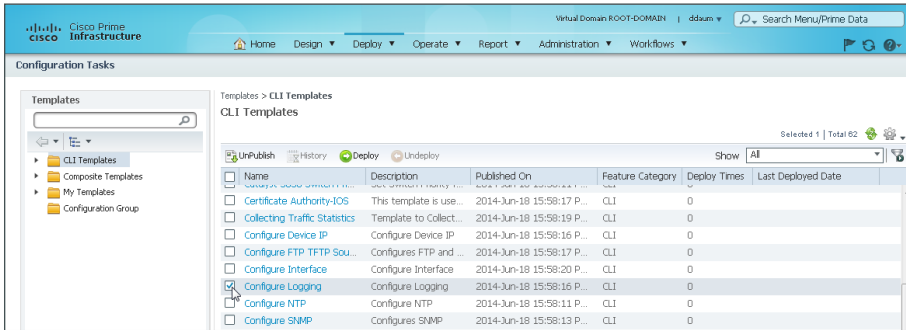
For more information about using the CleanAir templates, see the [Campus CleanAir Technology Design Guide](#).

The following procedure demonstrates how to use the CLI template for configuring logging on a managed switch.

Step 1: Navigate to **Deploy > Configuration Deployment > Configuration Tasks**.

The Configuration Tasks page shows tiles for all available templates.

Step 2: In the Templates tree, click **CLI Templates**, and then select the box next to **Configure Logging**.



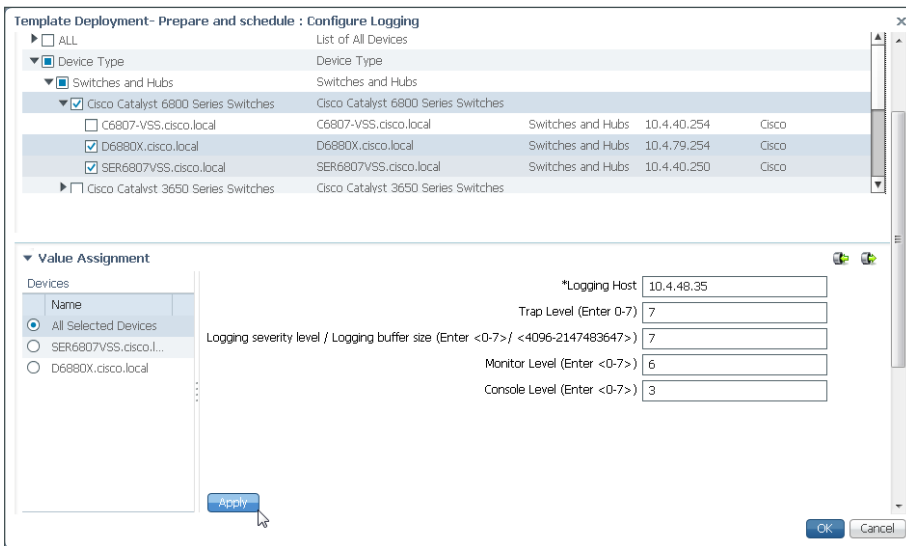
The **Deploy** button is activated for use.

Step 3: At the top of the list, click **Deploy**.

The Template Deployment dialog box appears.

Step 4: Under Device Selection, select the devices to which you want to deploy the template.

Step 5: Under Value Assignment, select specific devices or **All Selected Devices**, enter the required values, and click **Apply**.



Step 6: Under Schedule, enter a descriptive job name and select the start time.

Template Deployment- Prepare and schedule : Configure Logging

Console Level (Enter <0-7>) 3

Apply

▼ Schedule

Job Name Logging Configuration Deployment

Start Time Now Date 06/19/2014 09:43 AM (MM/dd/yyyy hh:mm AM/PM)

▼ Summary

Template **Configure Logging**

Deploy to number of devices 2

Deployment scheduled at: **2014-Jun-19 09:43:00 Eastern Standard Time**

OK Cancel

Step 7: Review your selections on the Template Deployment dialog box. When you are ready to submit the job, click **OK**.

At the selected start time, Cisco Prime Infrastructure applies the configuration template to the selected devices.



Tech Tip

To view the status of the job, navigate to **Administration > Jobs Dashboard** and look for the job name that you entered.

Appendix A: Product List

Network Management

| Functional Area | Product Description | Part Numbers | Software |
|--------------------|--|----------------|----------|
| Network Management | Cisco Prime Infrastructure 2.x | R-PI2X-K9 | 2.x |
| | Prime Infrastructure 2.1 Software | R-PI21-SW-K9 | 2.1 |
| | Prime Infrastructure 2.x Base License | L-PI2X-BASE | 2.x |
| | Prime Infrastructure 2.x - Lifecycle - 25 Device License | L-PI2X-LF-25 | |
| | Prime Infrastructure 2.x - Lifecycle - 50 Device License | L-PI2X-LF-50 | |
| | Prime Infrastructure 2.x - Lifecycle - 100 Device License | L-PI2X-LF-100 | |
| | Prime Infrastructure 2.x - Lifecycle - 500 Device License | L-PI2X-LF-500 | |
| | Prime Infrastructure 2.x - Lifecycle - 1K Device License | L-PI2X-LF-1K | |
| | Prime Infrastructure 2.x - Lifecycle - 2.5K Device License | L-PI2X-LF-2.5K | |
| | Prime Infrastructure 2.x - Lifecycle - 5K Device License | L-PI2X-LF-5K | |
| | Prime Infrastructure 2.x - Lifecycle - 10K Device License | L-PI2X-LF-10K | |
| | Prime Infrastructure 2.x - Lifecycle - 15K Device License | L-PI2X-LF-15K | |

Appendix B: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We revised the guide to show configurations using the updated software as shown in Appendix A: Product List.

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.

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.

© 2014 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)