






# Newer Cisco Validated Design Guides Available

This guide is part of an older series of Cisco Validated Designs.

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

-  [Open the latest version of this guide](#)
-  [Access the latest series of CVD Guides](#)
-  [Continue reading this archived version](#)





# Prime Infrastructure

## Technology Design Guide

April 2014



# Table of Contents

---

<b>Preface</b> .....	<b>1</b>
<b>CVD Navigator</b> .....	<b>2</b>
Use Cases .....	2
Scope .....	2
Proficiency.....	2
<b>Introduction</b> .....	<b>3</b>
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
<b>Deployment Details</b> .....	<b>7</b>
Installing and Configuring Cisco Prime Infrastructure.....	7
Managing the Network .....	31
<b>Appendix A: Product List</b> .....	<b>41</b>
<b>Appendix B: Changes</b> .....	<b>42</b>

# Preface

---

Cisco Validated Designs (CVDs) provide the foundation 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/campus>



# 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 following site:  
<http://www.cisco.com/go/cvd/campus>

# Introduction

---

Cisco Prime Infrastructure is a network management application capable of managing up to 10,000 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:

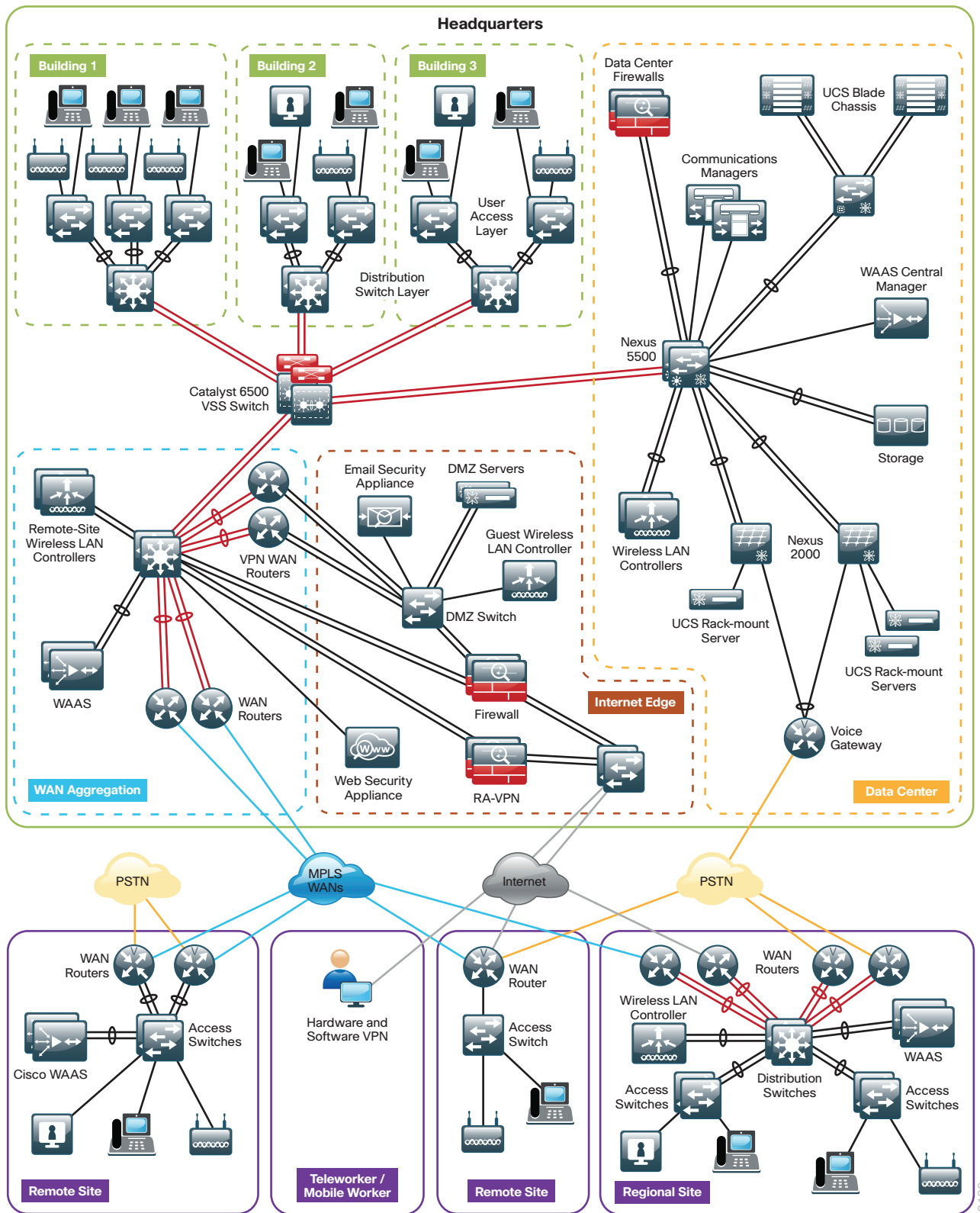
- **Configuration backup and archive**—Administrators need to make backup copies of device configurations and store them in a protected location. Performing this task manually is extremely time-consuming and tedious. An automated means of collecting and archiving device configuration files is an invaluable 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



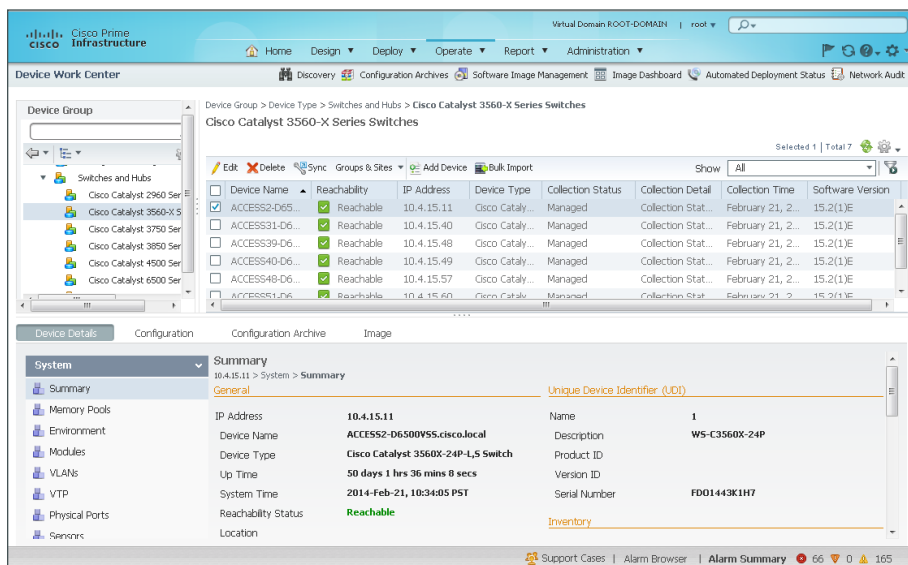
2169

## 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 out-of-the-box (OOTB) 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:

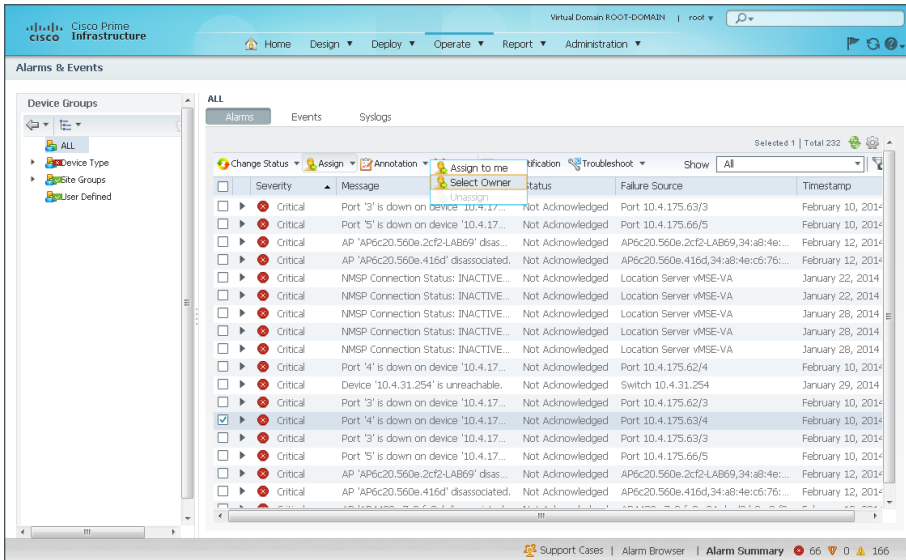
<http://velocity.apache.org/engine/devel/vtl-reference-guide.html>

## 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).



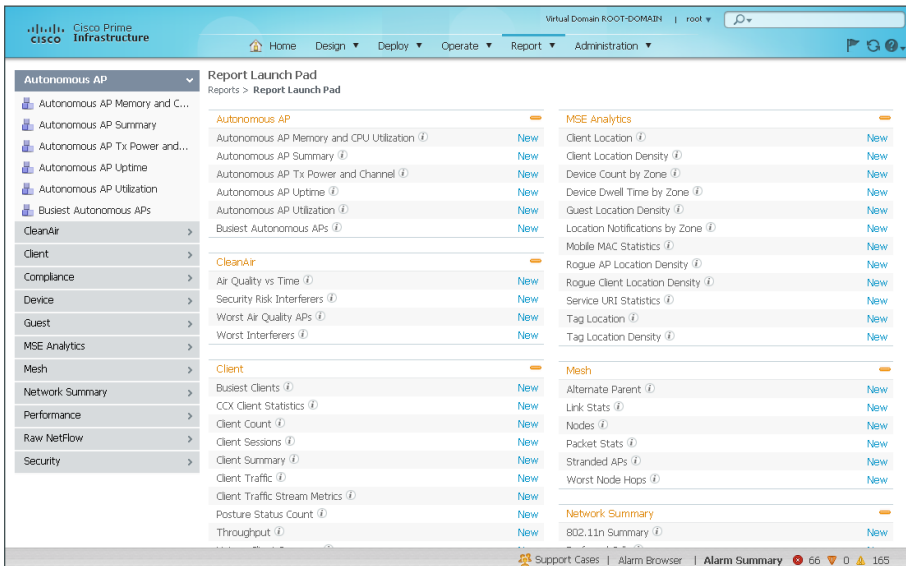
Figure 3 - Alarms and Events



## 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

## PROCESS

### Installing and Configuring Cisco Prime Infrastructure

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

Cisco Prime Infrastructure offers a single software installation that can manage up to 10,000 devices.

#### Procedure 1 Obtain a license

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.

You can acquire a license in one of two ways:

- If you are using physical media, complete Option 1.
- If you are downloading an evaluation version of the software, complete Option 2.

#### Option 1: Physical media

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](http://www.cisco.com) and log in.

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

[www.cisco.com/go/license](http://www.cisco.com/go/license)

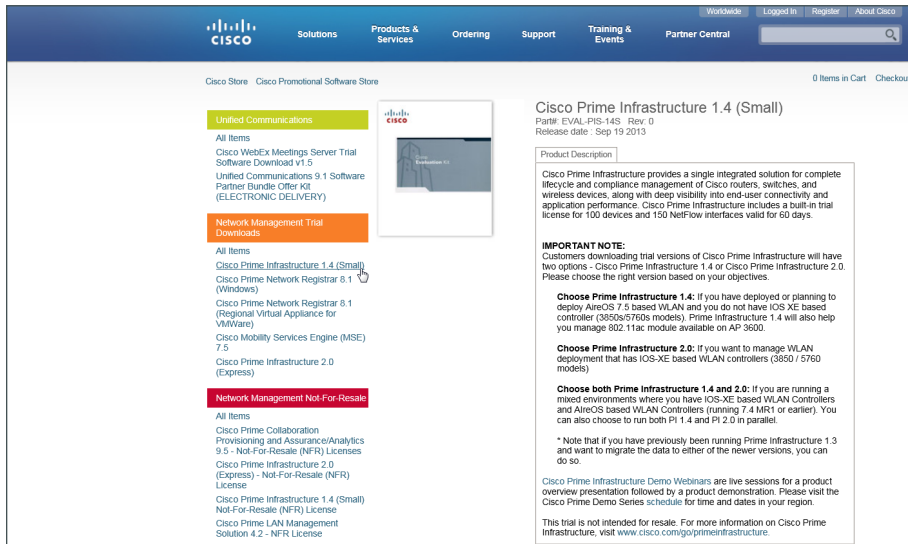
**Step 3:** If the **Continue to Product License Registration** button appears, click it.

**Step 4:** Enter the PAK that you were given.

## Option 2: Evaluation software

**Step 1:** Download an evaluation copy of Cisco Prime Infrastructure from the following site:

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



By email, you receive a PAK.

**Step 2:** In a web browser, go [www.cisco.com](http://www.cisco.com) and log in.

**Step 3:** In the address box of the browser window, enter:

[www.cisco.com/go/license](http://www.cisco.com/go/license)

**Step 4:** If the **Continue to Product License Registration** button appears, click it.

**Step 5:** Enter the PAK that you were given.

## Procedure 2 Install software

You can install the Cisco Prime Infrastructure 1.4.0.45 virtual appliance by using the Prime Infrastructure Open Virtualization Archive (OVA) image, and then applying the software update 1 to bring the 1.4.0.45 installation up to Prime Infrastructure version 1.4.1.

Before installing, please note the following:

- 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 30 minutes
  - Virtual-environment installation—Approximately 50 minutes
- Soft appliance OVA software can be installed only in a VMware environment.



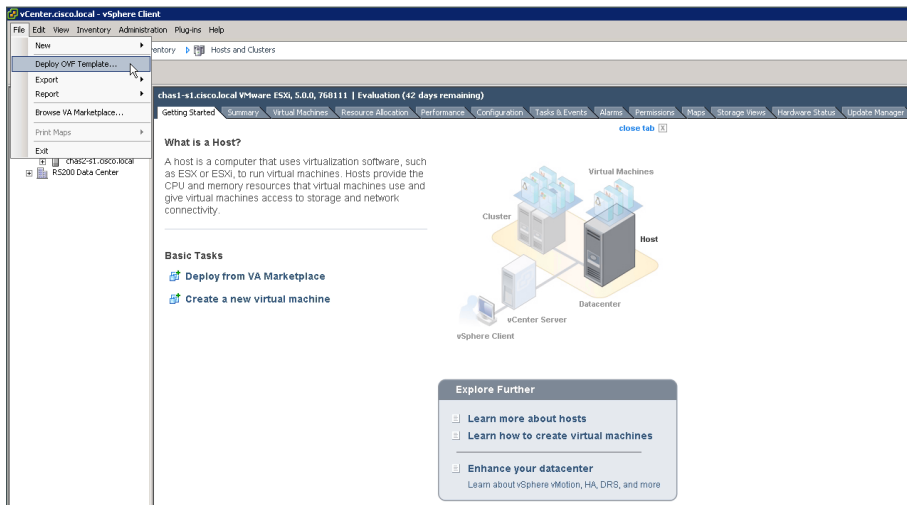
## Tech Tip

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.

It is recommended you do the following before installing the Cisco Prime Infrastructure 1.4.0.45 soft appliance:

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

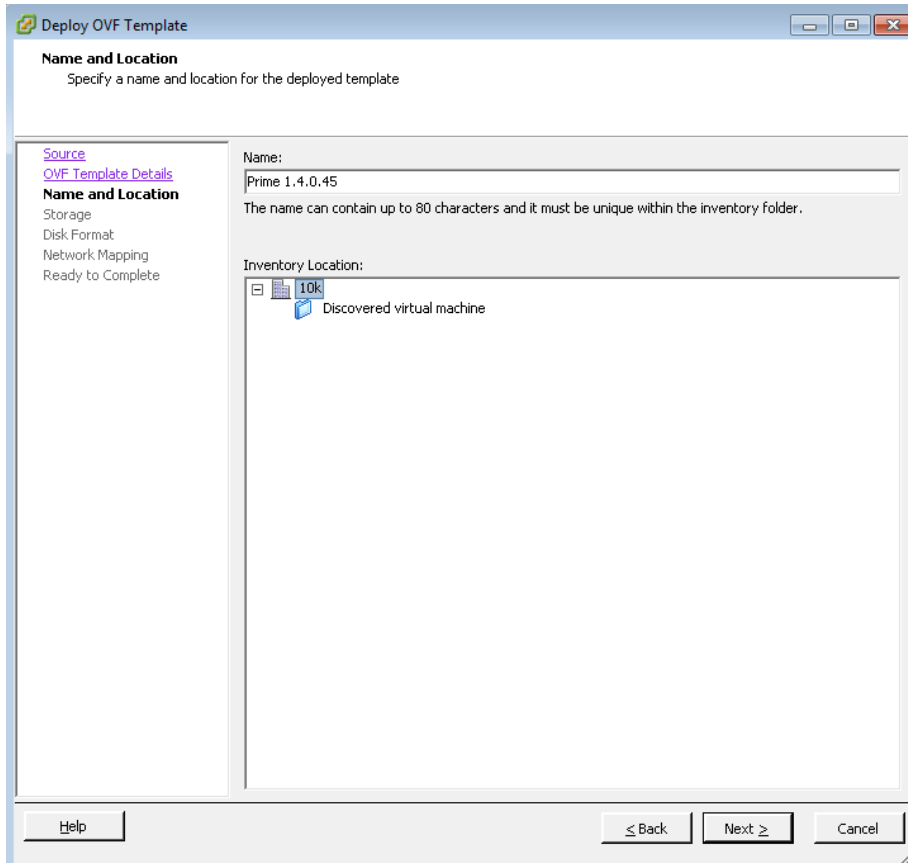
**Step 1:** In the VMware vSphere client, click **File** and then choose **Deploy OVF Template**.



**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-1.4.0.45), choose a location to install the virtual appliance, and then click **Next**.



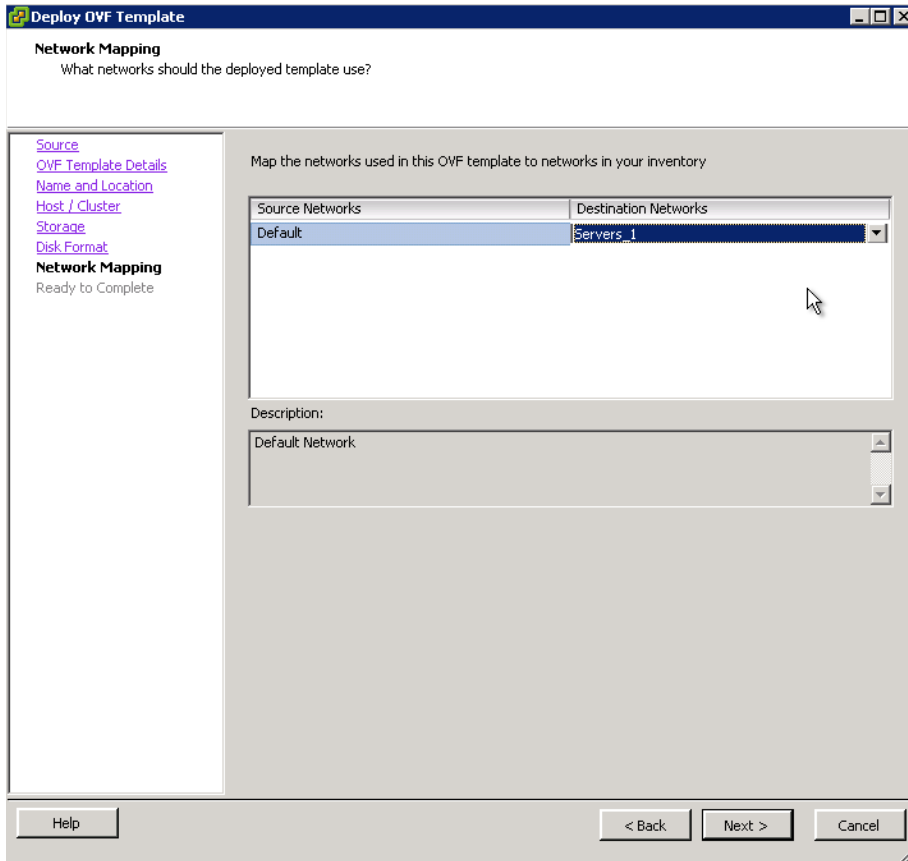
**Step 5:** On the Host/Cluster page, choose the host or cluster on which to install this virtual machine and then click **Next**.

**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 1.4.0.45 begins.

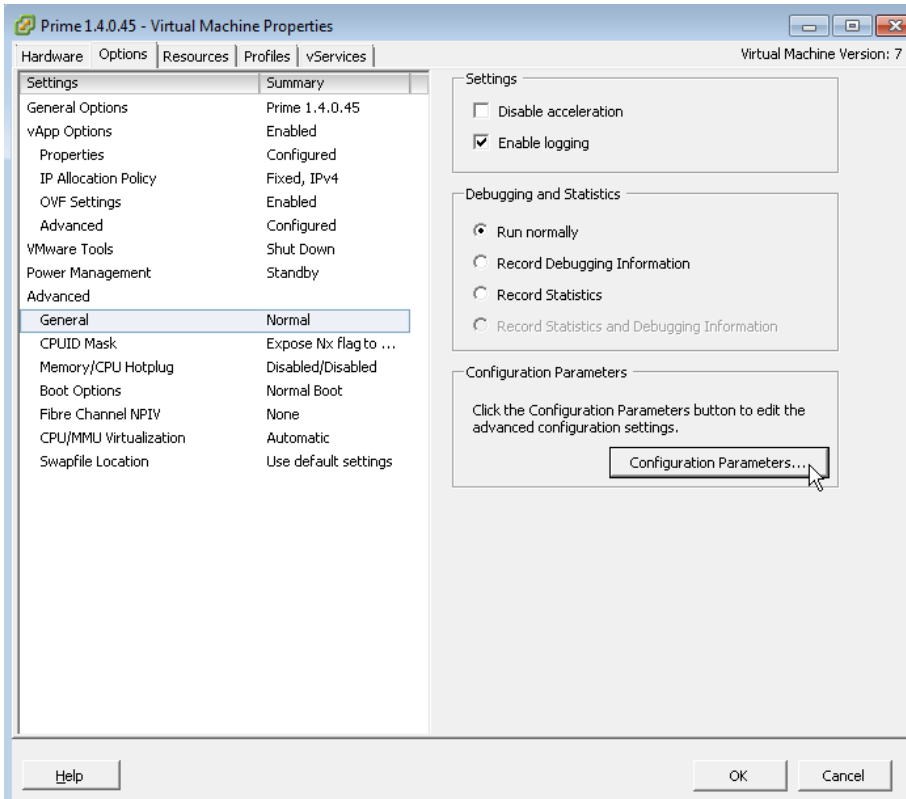
### Procedure 3 Customize the VMware environment

#### (Optional)

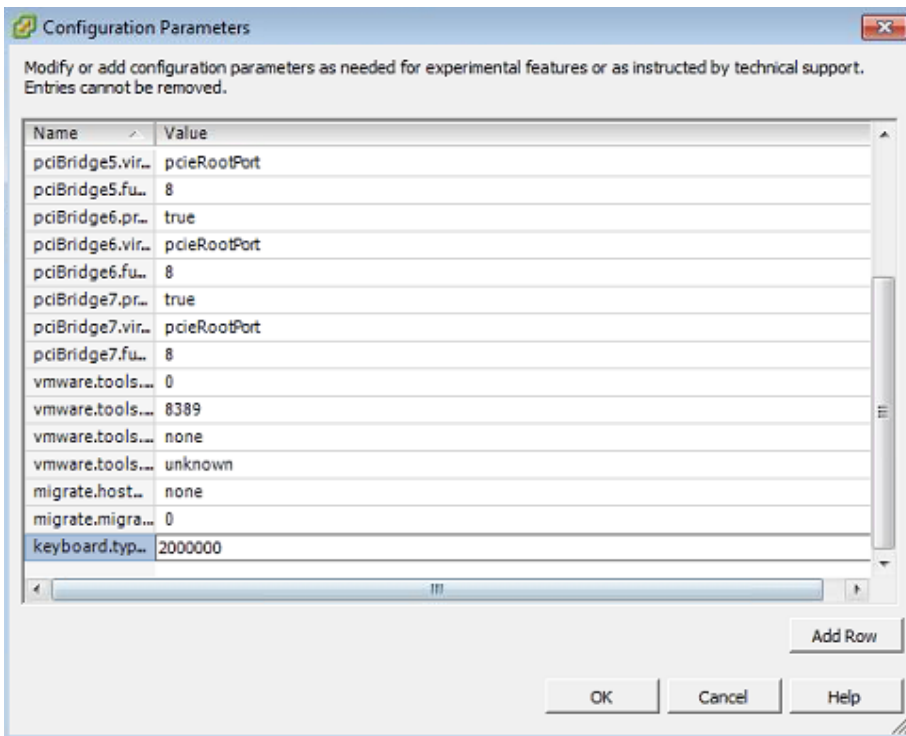
If you find that key strokes are repeating when entering various settings, it may be necessary to configure a keyboard delay value. This procedure is optional but is included here in the event that it is required.

**Step 1:** Using the VMware vSphere client, access the VMware vCenter environment, 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, 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**.

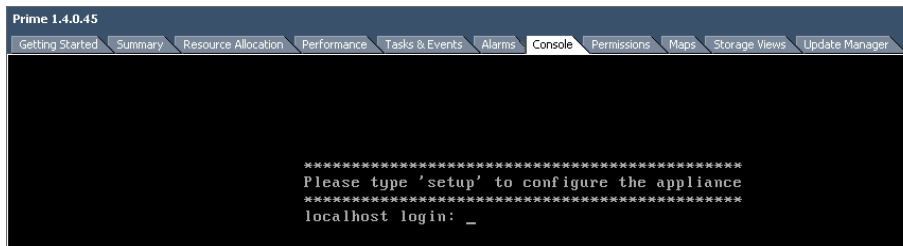


**Step 4:** On the Virtual Machine Properties dialog box, click **OK**.

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

## Procedure 4 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.

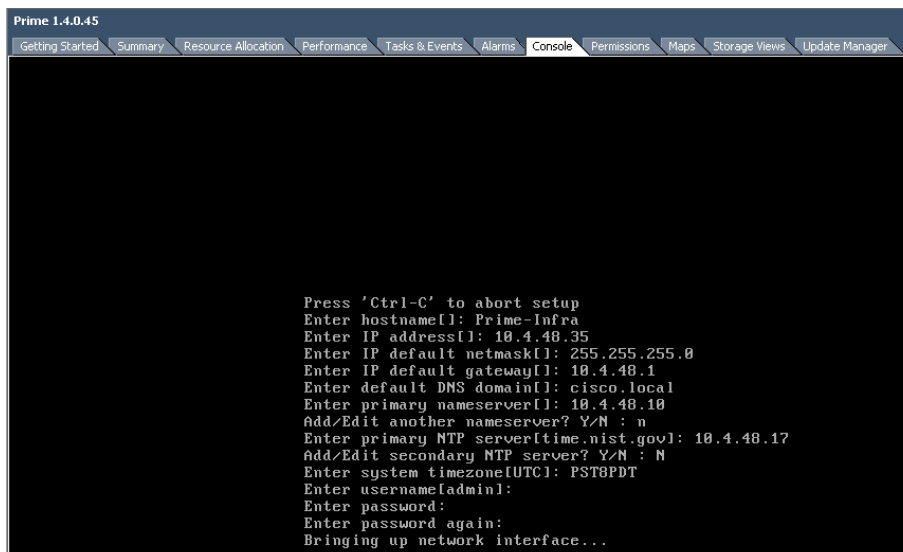


```
Prime 1.4.0.45
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views Update Manager

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

**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**



```
Prime 1.4.0.45
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views Update Manager

Press 'Ctrl-C' to abort setup
Enter hostname[]: Prime-Infra
Enter IP address[]: 10.4.48.35
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.4.48.1
Enter default DNS domain[]: cisco.local
Enter primary nameserver[]: 10.4.48.10
Add/Edit another nameserver? Y/N : n
Enter primary NTP server[time.nist.gov]: 10.4.48.17
Add/Edit secondary NTP server? Y/N : N
Enter system timezone[UTC]: PST8PDT
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface...
```

**Step 3:** 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.

```
Prime 1.4.0.45
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views Update Manager

Press 'Ctrl-C' to abort setup
Enter hostname[]: Prime-Infra
Enter IP address[]: 10.4.48.35
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.4.48.1
Enter default DNS domain[]: cisco.local
Enter primary nameserver[]: 10.4.48.10
Add/Edit another nameserver? Y/N : n
Enter primary NTP server[time.nist.gov]: 10.4.48.17
Add/Edit secondary NTP server? Y/N : N
Enter system timezone[UTC]: PST8PDT
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use 'Ctrl-C' from this point on...
Appliance is configured
Installing applications...
Installing MCS ...
```

**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**.

```
Prime 1.4.0.45
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views Update Manager

Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use 'Ctrl-C' from this point on...
Appliance is configured
Installing applications...
Installing MCS ...
Prime Infrastructure Application installation completed
Install Completed Successfully
find: /storeddata/Installed: No such file or directory
Application Install Completed.

Post-install Process Started...

Post-install Version Validation Process Started...
*****
* Cisco Prime Infrastructure Setup *
*****
Enter "~" to return to previous question.

*****
* High Availability Role Selection *
*****
Will this server be used as a Secondary for HA? (yes/no):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.

```
Prime 1.4.0.45
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views Update Manager

*****
* Web Interface Root Password Selection *
*****
Enter root password:
Enter root password again:
The system admin password cannot contain 'cisco' or 'ocsic', or any variant obtained by changing the capitalization of letters therein or by substituting '1', 'l', or 't' for i, '0' for 'o', or '$' for 's'.
Enter root password:
Enter root password again:

*****
* FTP Password Selection *
*****
Enter ftp password:
Enter ftp password again:

*****
* Summary *
*****
Server will not be a Secondary
Root Password is set.
Ftp Password is set.
Apply these settings? (y/n)█
```

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

```
Prime 1.4.0.45
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views Update Manager

l', or 't' for i, '0' for 'o', or '$' for 's'.
Enter root password:
Enter root password again:

*****
* FTP Password Selection *
*****
Enter ftp password:
Enter ftp password again:

*****
* Summary *
*****
Server will not be a Secondary
Root Password is set.
Ftp Password is set.
Apply these settings? (y/n)y
Settings Applied.

Application bundle (NCS) installed successfully
=== Initial Setup for Application: NCS ===

Running database cloning script...█
```

## Procedure 5 Apply software update

You upgrade Cisco Prime Infrastructure from version 1.4.0.45 to version 1.4.1 by applying the software upgrade patch.

**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 1.4.0.45 installation. Login using the admin username and password created during the initial installation. (Example: admin/C1sco123)

**Step 3:** Enter configuration mode.

```
Prime-Infra/admin# config term  
Enter configuration commands, one per line. End reend  
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
```

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

```
Prime-Infra/admin# show repository My-Prime-Repository  
PI_1.4_0_45_Update_1-39.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_1.4_0_45_Update_1-39.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 version 1.4.1 but instead only shows the base version of 1.4. The **show version** command is the only way to verify that patch 1 has been applied to the base 1.4 installation.

```
Prime-Infra/admin# show version
Cisco Application Deployment Engine OS Release: 2.0
ADE-OS Build Version: 2.0.1.038
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 Network Control System
-----
Version : 1.4.0.45
Patch: Cisco Prime Network Control System Version:
Update-1_39_for_version_1_4_0_45
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. This is documented in the [Cisco Prime 1.4.1 release notes](#).

**Step 11:** If you want the host name to reflect the version of Cisco Prime Infrastructure installed, rename the VM Host in VMware (Example: Prime 1.4.1).

### Procedure 6 Configure browser settings

Cisco Prime Infrastructure supports the following browsers:

- Google Chrome—25.0, 26.0 or 27.0
- Mozilla Firefox— ESR 17.x, 17.0 or later
- Microsoft Internet Explorer—8.0 or 9.0 with Chrome plug-in (native Internet Explorer is not supported)

The recommended minimum resolution is 1280 x 800 pixels.

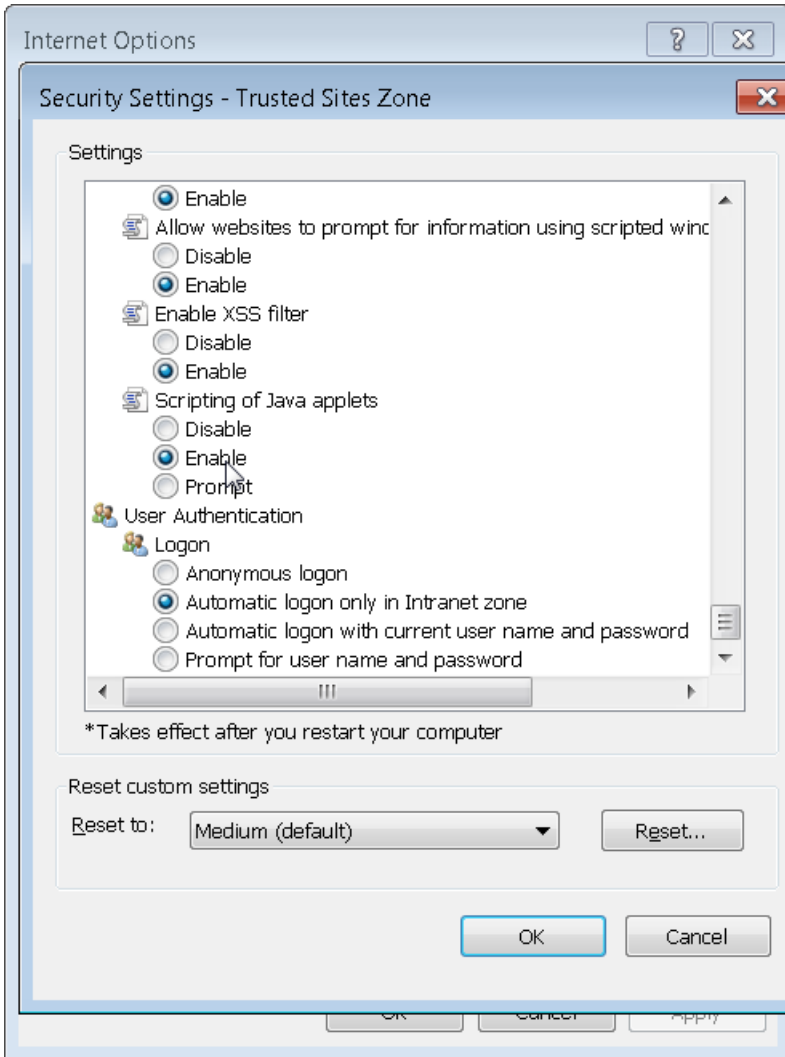
For the latest information about supported browsers, see the [Cisco Prime Infrastructure release notes](#).

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

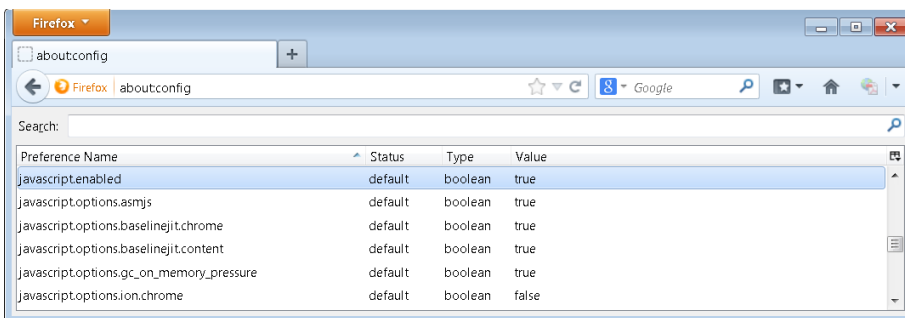
Some browsers allow you to enter the IP or hostname of specific sites that pop-up blocking should be disabled for. This approach allows pop-up blocking to be allowed globally with only those sites enter to be excluded.

**Step 2:** Enable JavaScript.

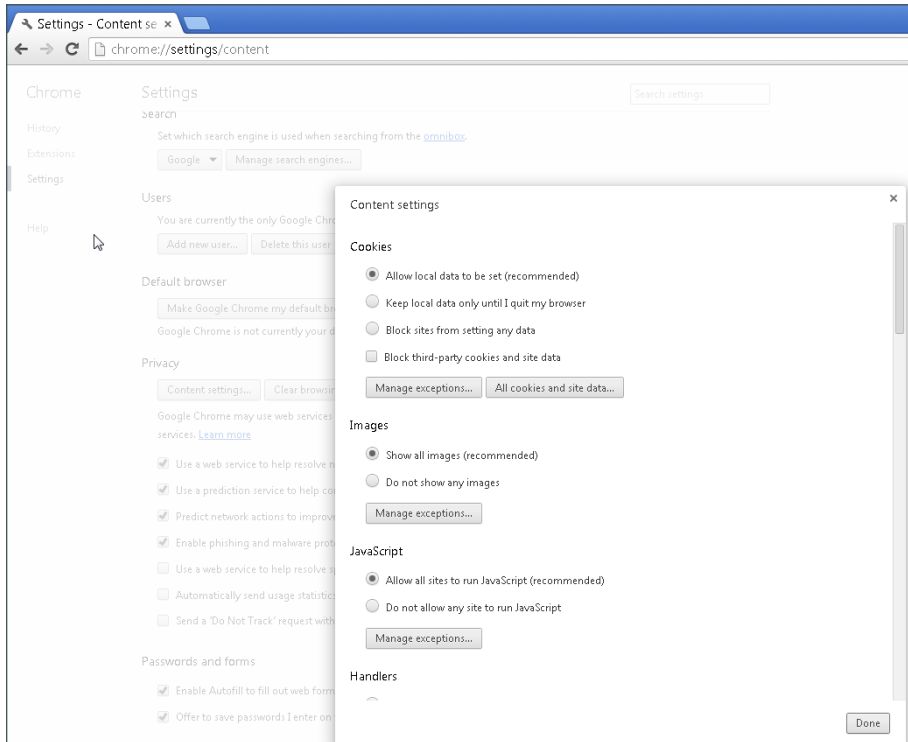
If you are using Internet Explorer 8 or later, navigate to **Tools > Internet Options > Security > Custom level > Settings**, and then under **Scripting of Java applets**, select **Enable**.



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**.



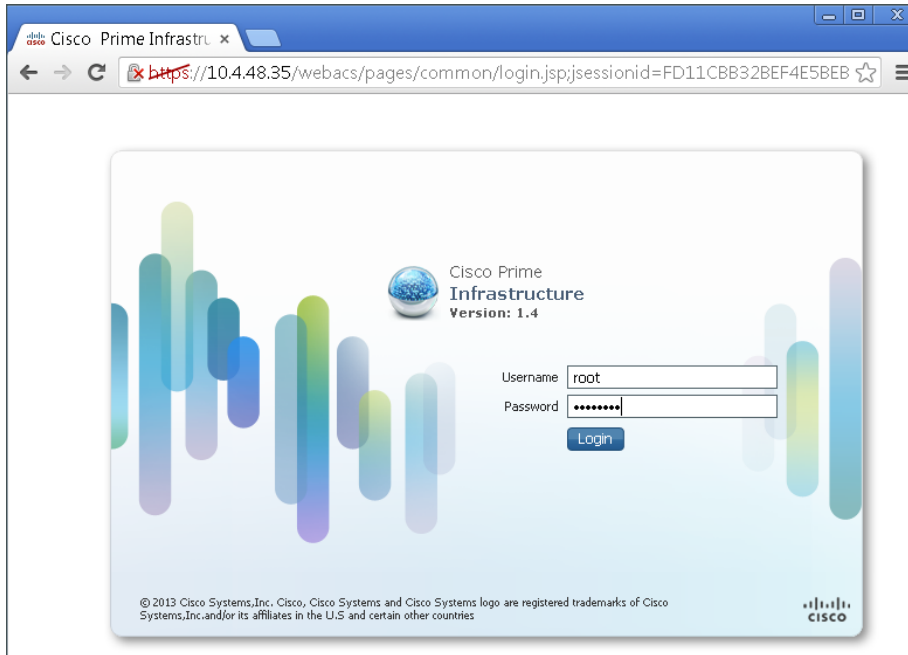
If you are using Chrome 25.0 or later, enter **chrome://settings/content** in the navigation bar and verify that JavaScript is enabled.



## Procedure 7 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>).

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



### Tech Tip

The version displayed on the web interface will not reflect version 1.4.1. This is normal. To verify the version, use SSH to connect to the Cisco Prime Infrastructure installation and enter the **show version** command, as described in Step 10 in Procedure 5.

**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.

### Mail Server Configuration

Administration > System Settings > Mail Server Configuration

#### Primary SMTP Server

Hostname/IP	<input type="text" value="smtp.cisco.local"/>	Port	<input type="text" value="25"/>
Username (Optional)	<input type="text"/>		
Password	<input type="text"/>		
Confirm Password	<input type="text"/>		

#### Secondary SMTP Server (Optional)

Hostname/IP	<input type="text"/>	Port	<input type="text" value="25"/>
Username (Optional)	<input type="text"/>		
Password	<input type="text"/>		
Confirm Password	<input type="text"/>		

#### Sender And Receivers

From	<input type="text" value="PI@Prime-Infra.cisco.local"/>
To	<input type="text" value="johnsmith@thiscompany.com"/> <small>comma-separated email addresses</small>
<input checked="" type="checkbox"/> Apply recipient list to all existing alarm email notifications.	
Subject	<input type="text"/> <small>This text will be appended to the email subject</small>

[Configure email notification for individual alarm categories.](#)

## Procedure 8 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.

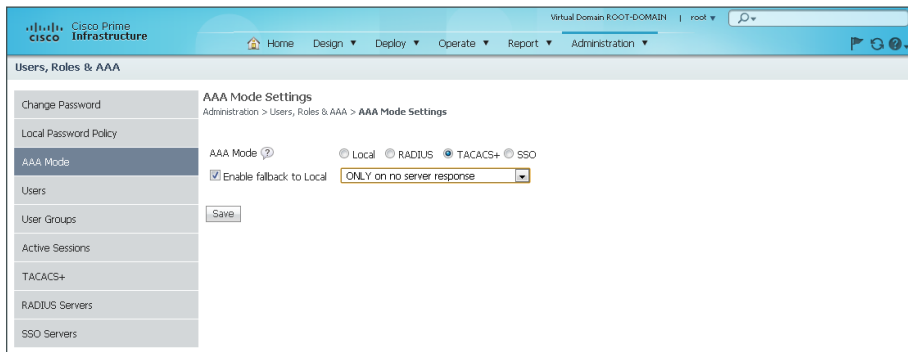
**Step 1:** Navigate to **Administration > Users, Roles & AAA**, and then click **AAA Mode**.

The AAA Mode Settings page appears.

**Step 2:** Select **TACACS+**.

**Step 3:** Select the **Enable fallback to Local** option and then in the list, choose **ONLY on no server response**.

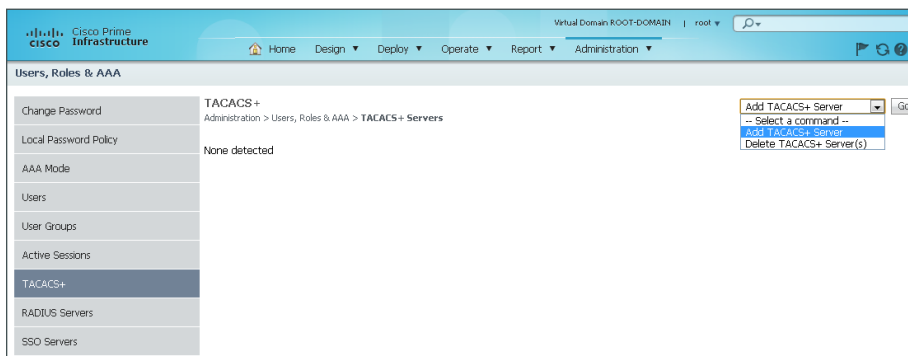
**Step 4:** Click **Save**.



**Step 5:** In the left column, click **TACACS+**.

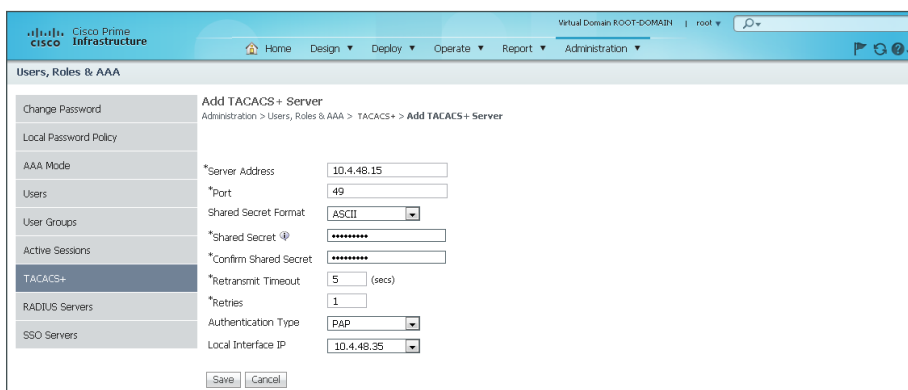
The TACACS+ page appears.

**Step 6:** In the **Select a command** list in the upper right corner of the web page, choose **Add TACACS+ Server**, and then click **Go**.



**Step 7:** In the **Server Address** box, enter the IP address of the TACACS+ server (Example: 10.4.48.15)

**Step 8:** In the **Shared Secret** and **Confirm Shared Secret** boxes, enter the secret key (Example: SecretKey), and then click **Save**.



## Procedure 9 Configure users and user groups

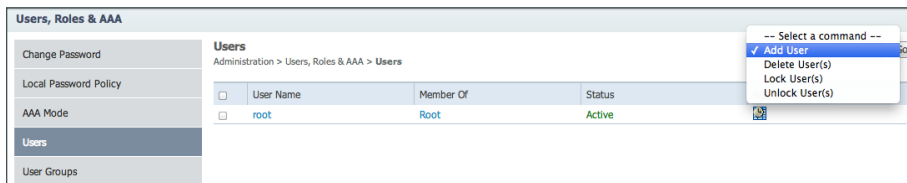
*User groups (or roles)* are collections of privileges that dictate the type of system access the user has. Some predefined roles are:

- **System Monitoring**—These 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 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**.

**Users, Roles & AAA**

**Add User**  
Administration > Users, Roles & AAA > Users > Add User

**General** Virtual Domains

Username

New Password

Confirm Password

Groups Assigned to this User

- Admin
- Config Managers
- Lobby Ambassador
- Monitor Lite
- North Bound API
- Root
- Super Users
- System Monitoring
- User Assistant
- User Defined 1

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

## Procedure 10 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:

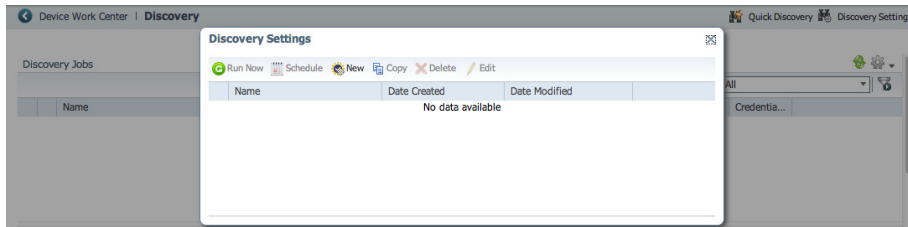
<http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/index.html>

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

**Step 1:** Navigate to **Operate > 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.

A screenshot of the blank Discovery Settings dialog box. The dialog box is titled "Discovery Settings" and has a close button in the top right corner. The "Current Discovery Settings" section is visible. The "Protocol Settings" section includes a "PingSweep Module" dropdown menu with a plus sign, and two expandable sections: "Layer 2 Protocols" and "Advanced Protocols". The "Filters" section includes an "IP Filter" dropdown menu with a plus sign and an expandable section: "Advanced Filters". The "Credential Settings" section includes four credential dropdown menus: "SnmpV2 Credential", "Telnet Credential", "SSH Credential", and "SnmpV3 Credential", each with a plus sign. The "Preferred Management IP" section includes a dropdown menu with "Use Loopback" selected. At the bottom right, there are three buttons: "Save", "Run Now", and "Cancel".



**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**.

**Step 7:** Click **Add Row**.

**Step 8:** In the **Seed Device** box, enter the management IP address for the core switch (Example: 10.4.40.49), and then below the Seed Device box, click **Save**.



### Tech Tip

If you leave the Hop Count column blank, the discovery process continues until the end neighbor is reached. Depending on the network size, this could be a large number of network devices. In large networks, it is recommended that you add a Hop Count value to restrict the size of the discovery.

**Discovery Settings** [X]

\*Name  **Current Discovery Settings**  
CDP Module ⊕

**Protocol Settings**  
PingSweep Module ⊕

▼ **Layer 2 Protocols**

CDP Module

Enable Cisco Discovery Protocol  
 Enable Cross Router Boundry

Edit Delete Add Row Import CSV File ⊕

Seed Device	Hop Count
<input checked="" type="radio"/> 10.4.40.53	
<input type="radio"/> 10.4.40.49	

Save | Cancel

SSH Credential ⊕  
SnmpV3 Credential ⊕

**Preferred Management IP**  
Use Loopback ▼

Save Run Now Cancel

**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/write community string (Example: cisco123).

**Step 14:** Repeat the preceding three steps and add a second row using the read only community string (Example: cisco)

**Step 15:** Below the IP box, click **Save**.

The screenshot shows the 'Discovery Settings' dialog box. The 'Name' field is 'My\_Discovery\_Settings'. Under 'Protocol Settings', 'PingSweep Module' is selected. Under 'Layer 2 Protocols', 'CDP Module' and 'LLDP Module' are selected. Under 'Filters', 'IP Filter' is selected. In the 'Credential Settings' section, 'SnmpV2 Credential' is expanded, and the checkbox 'Enable SnmpV2 Credential' is checked. Below this, there are 'Edit', 'Delete', and 'Add Row' buttons. A table shows one row with the following data:

IP	Read Community String	Snmp Timeout	Snmp Retry
*.*.*	*****	3	2

### Tech Tip

Adding the read/write community string is critical 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 16:** Next to SSH Credential, click the + icon.

**Step 17:** Select **Enable ssh Credential**.

**Step 18:** Click **Add Row**.

**Step 19:** 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 20:** Enter the username, password, and enable password.

**Step 21:** Select **SSHv2**, and then below the User Name box, click **Save**.

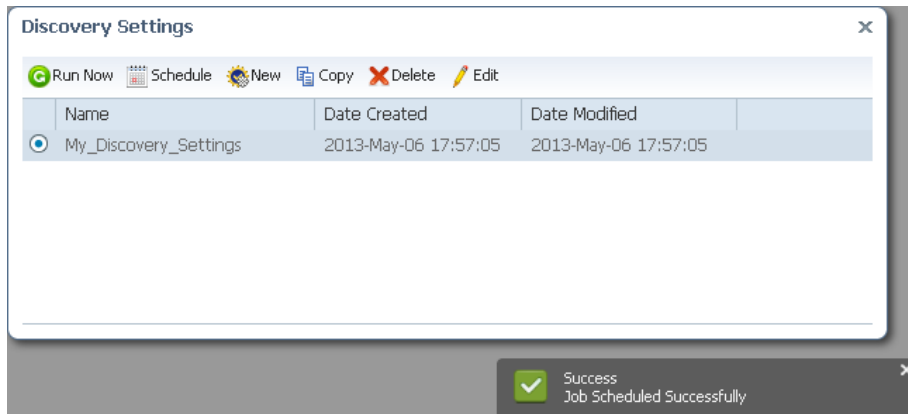
The screenshot shows a 'Discovery Settings' dialog box with the following sections:

- \*Name:** My\_Discovery\_Settings
- Current Discovery Settings:** CDP Module (+), SnmpV2 Credential (+), SSH Credential (+)
- Protocol Settings:** PingSweep Module (+)
- Layer 2 Protocols:** CDP Module (+), LLDP Module (+)
- Advanced Protocols:** (collapsed)
- Filters:** IP Filter (+)
- Advanced Filters:** (collapsed)
- Credential Settings:** SnmpV2 Credential (+), Telnet Credential (+), SSH Credential (-)
- Enable ssh Credential
- Actions:** Edit, Delete, Add Row
- Table:**

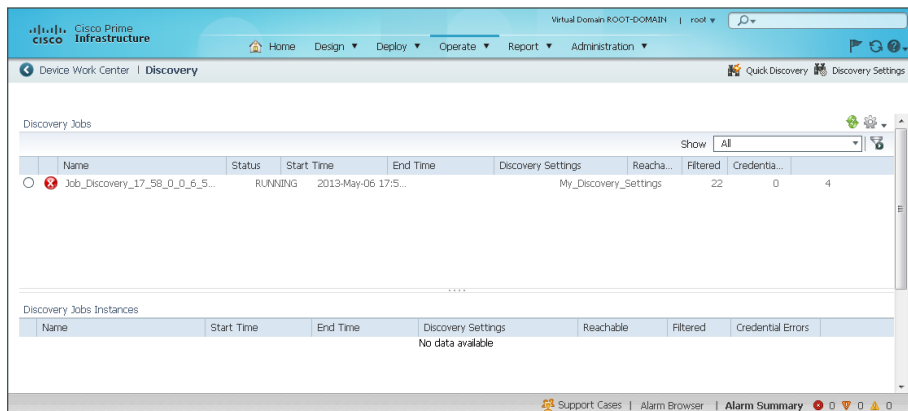
IP	User Name	Password	Enable Passw...	SSH Version
*.*.*.*	*****	*****	*****	SSHV2

## Step 22: Click Run Now.

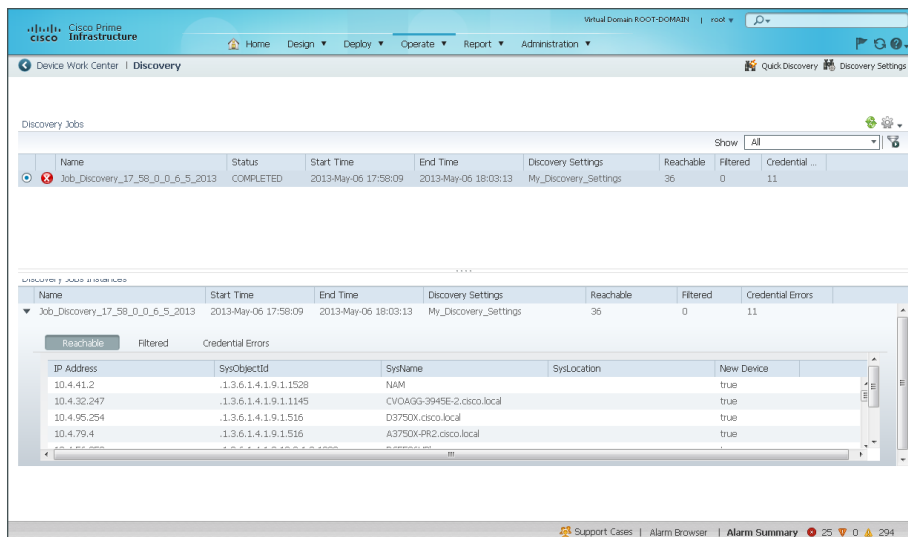
The discovery settings are saved and Cisco Prime Infrastructure begins device discovery. The amount of time this discovery process takes depends on the number of devices on the network.



**Step 23:** 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 11 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.

**Step 1:** Navigate to **Administration > System Settings** and then 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:** Ensure that **TFTP fallback** is not selected.

**Step 4:** Select **Use SCP for image upgrade and import**. If it is not selected, Cisco Prime Infrastructure does not use SCP for image distribution, regardless of the selected protocols in the Image transfer protocol order list.

**Step 5:** 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 6:** 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 7:** Click **Save**.

## Procedure 12 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 out-of-the-box configuration template to configure logging on devices. For an example of using the logging configuration template, see the [Deploy out-of-the-box templates procedure](#).

**Step 1:** Navigate to **Administration > Logging** and then click **SysLog Logging Options**. The SysLog Logging Options page appears.

The screenshot shows the Cisco Prime Infrastructure web interface. The top navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', and 'Administration'. The 'Administration' menu is expanded to show 'Logging'. On the left, a sidebar lists 'General Logging Options', 'SNMP Logging Options', and 'SysLog Logging Options'. The main content area is titled 'SysLog Logging Options' and shows the breadcrumb 'Administration > Logging > SysLog Logging Options'. Below this, there is a 'SysLog Settings' section with a 'Save' button at the bottom. The settings include: 'Enable SysLog' with a checked 'Enable' checkbox; 'SysLog Host' with a text input field containing '10.4.48.35'; and 'SysLog Facility' with a dropdown menu set to 'LOCAL7'.

**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 out-of-the-box 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.



## 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.

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

**Step 1:** Navigate to **Operate > 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: CAT2960S

Select Image Version: 15.2.1E1

Select Feature Package: UNIVERSAL

Selected Image: c2960s-universalk9-mz.152-1.E1.bin

---

▼ Schedule

Job Name: CCO\_Image\_Collection\_C2960S\_15\_31\_39\_56\_14\_1\_2014

Start Time:  Now  Date 02/14/2014 03:32 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](http://www.cisco.com), login with the credentials that you provided in Procedure 11, 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**.

<input type="checkbox"/>	File Name	Image Family
<input type="checkbox"/>	AIR-CT5500-K9-7-6-100-0.aes	WLC
<input checked="" type="checkbox"/>	c2960s-universalk9-mz.152-1.E1.bin	C2960S

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	
▶ <b>Device Selection</b>	
▶ <b>Distribute Image and Location Selection</b>	
▶ <b>Distribution Options</b>	
▼ <b>Schedule Distribution</b>	
Job Name	<input type="text" value="A2960S_95_9_1521E_14_40_38_252_15_1_2014"/>
Start Time	<input checked="" type="radio"/> Now <input type="radio"/> Date <input type="text" value="02/15/2014 02:41 PM"/> (MM/dd/yyyy hh:mm AM/PM)

**Step 14:** Click **Submit**.

Cisco Prime Infrastructure begins the software image distribution job.



### 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 > Performance**.

The monitoring page displays the performance monitoring dashboard.

**Step 2:** If Network Device 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.

Device Name	Device IP	Average	Maximum	Minimum	Current
ACCESS31-D6500VSS.cisco.local	10.4.15.40	37%	37%	37%	37%
ACCESS39-D6500VSS.cisco.local	10.4.15.48	34%	34%	33%	34%
ACCESS41-D6500VSS.cisco.local	10.4.15.50	33%	33%	32%	32%
A2960S-D4507.cisco.local	10.4.95.9	32%	97%	9%	11%
ACCESS38-D6500VSS.cisco.local	10.4.15.47	32%	33%	31%	33%

**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.

Top N CPU Utilization

Dashlet Title: Top N CPU Utilization

Refresh Dashlet:

Refresh Interval: 5 minutes

Time Filter Lock:

No. of Rows: 5 (Default)

Device Family: ALL

Time Frame:  Past 1 hour

Buttons: Reset, Save, Save And Close, Close

Device Name	Device IP	Average	Maximum	Minimum	Current
ACCESS31-D6500VSS.cisco.local	10.4.15.40	37%	37%	37%	37%
ACCESS39-D6500VSS.cisco.local	10.4.15.48	34%	34%	33%	34%
ACCESS41-D6500VSS.cisco.local	10.4.15.50	33%	33%	32%	32%
A2960S-D4507.cisco.local	10.4.95.9	32%	97%	9%	11%
ACCESS38-D6500VSS.cisco.local	10.4.15.47	32%	33%	31%	33%

**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:** Scroll down to the Device category and click **Inventory**.

Device	
AP Image Pre-download ⓘ	New
AP Profile Status ⓘ	New
AP Summary ⓘ	New
Busiest APs ⓘ	New
CPU Utilization ⓘ	New
Classmap QOS Statistics ⓘ	New
Detailed Device Inventory ⓘ	New
Device Health ⓘ	New
Dmvpn Reports ⓘ	New
GET VPN Network Status ⓘ	New
Identity Capability ⓘ	New
Interface Availability ⓘ	New
Interface Utilization ⓘ	New
<u>Inventory</u> ⓘ	New
License By Device Type ⓘ	New

**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.
- **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.

Settings	
<input type="checkbox"/>	<b>Create reports in current and each sub Virtual Domains</b> ⓘ <a href="#">View sub Virtual Domains</a>
Report Title	Switch Inventory
Report Type	Switches
Customize Report	<input type="button" value="Customize"/> <b>Customize the data for this report</b>

**Step 5:** Click **Customize**.

**Step 6:** In the **Report View** list, choose whether the report should contain tables, charts, or both.

**Step 7:** If you want to add or remove fields from the report, in the Custom Report Name list, choose the subreport that includes the fields and then use the Add and Remove buttons to configure the “Data fields to include” list.

Custom Report Name:   Do not include

**Available data fields**

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

**Data fields to include**

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

\* Blue fields are mandatory in this subreport.

Data field sorting

Sort by:   Ascending  Descending

Then by:   Ascending  Descending

Then by:   Ascending  Descending

Then by:   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 8:** Click **Apply**.

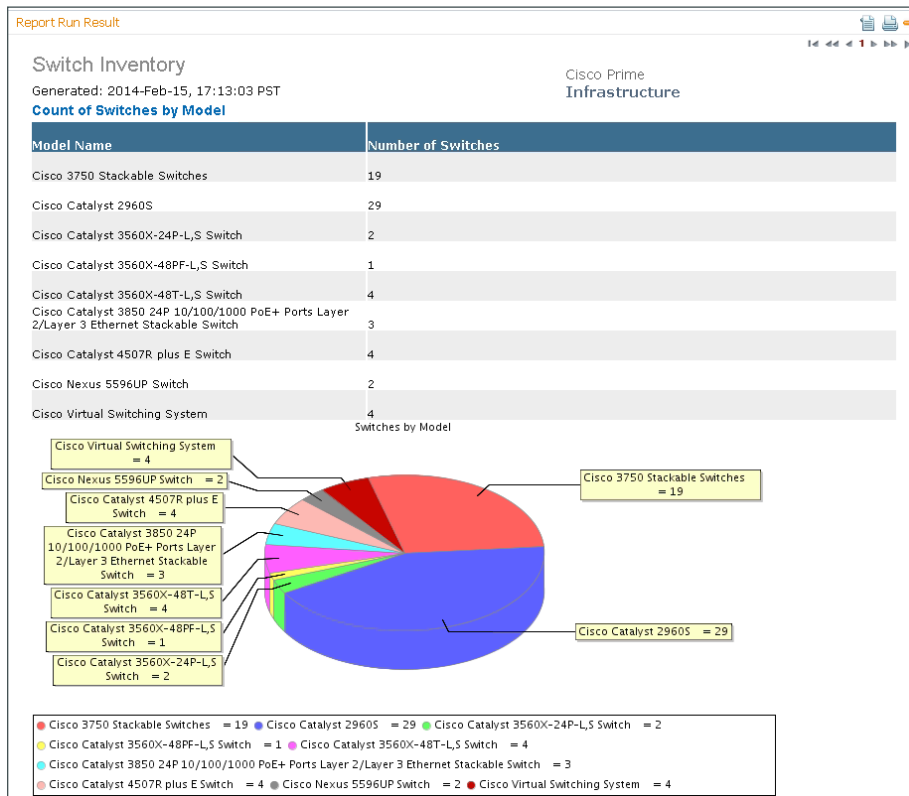
**Step 9:** If you want the report to run at a specific time, under Schedule,

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

**Step 10:** 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 11:** 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 out-of-the-box 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 out-of-the-box (OOTB) 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](#).

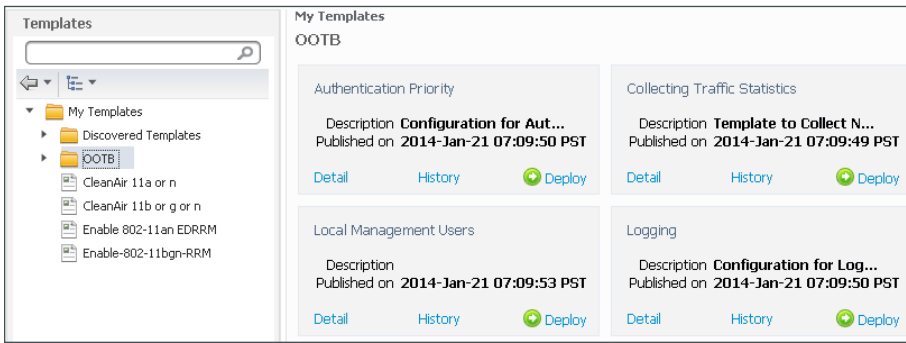
The following procedure demonstrates how to use the OOTB template for configuring logging on a managed switch.

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

The Configuration Tasks page shows tiles for all available templates.

**Step 2:** In the Templates tree, expand **My Templates** and click **OOTB**.

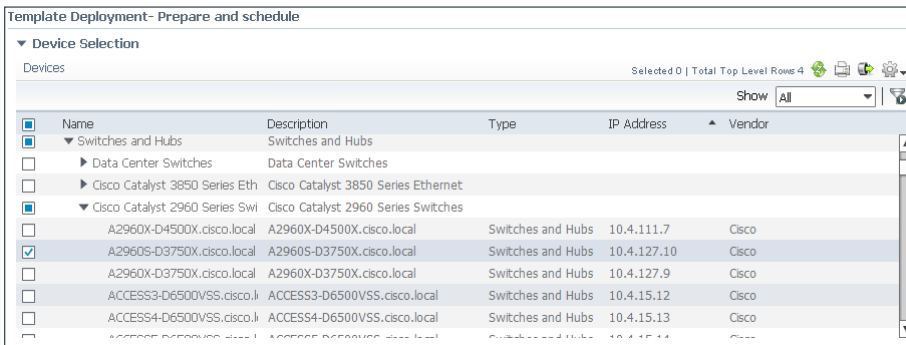
The Configuration Tasks page shows tiles only for the out-of-the-box templates.



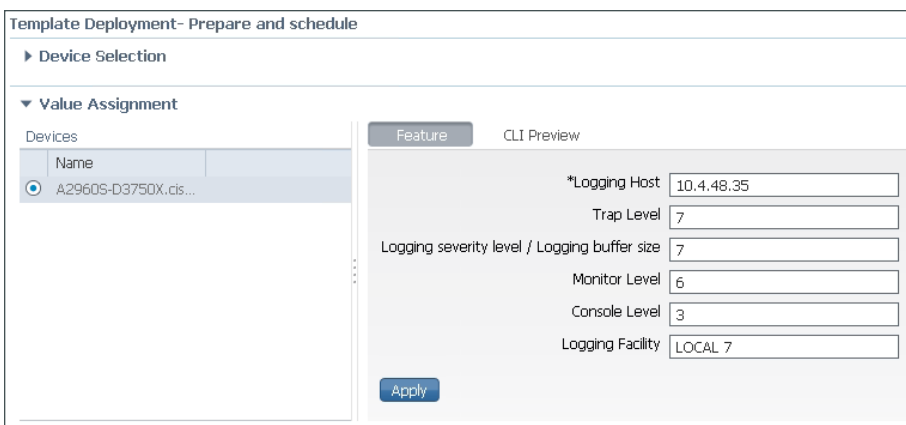
**Step 3:** In the tile for template that you want to deploy, click **Deploy**.

The Template Deployment dialog box appears.

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



**Step 5:** For each device that you selected in the previous step, under Value Assignment, select the device, enter the required values, and click **Apply**.





## Tech Tip

If you want to see the CLI commands that the template will apply to the device selected under Value Assignment, click the **CLI Preview** tab.

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

**Template Deployment- Prepare and schedule**

---

▶ **Device Selection**


---

▶ **Value Assignment**

---

▼ **Schedule**

Job Name

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

**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 1.2	R-PI12-K9 <sup>†</sup>	1.4.1 <sup>†</sup> PI_1_2-CSCum71308-0
	Cisco Prime Infrastructure 1.2 Base License and Software	R-PI12-BASE-K9 <sup>†</sup>	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 25 Device License	L-PI12-LF-25 <sup>†</sup>	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 50 Device License	L-PI12-LF-50 <sup>†</sup>	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 100 Device License	L-PI12-LF-100 <sup>†</sup>	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 500 Device License	L-PI12-LF-500 <sup>†</sup>	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 1000 Device License	L-PI12-LF-1K <sup>†</sup>	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 2500 Device License	L-PI12-LF-2.5K <sup>†</sup>	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 5000 Device License	L-PI12-LF-5K <sup>†</sup>	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 10,000 Device License	L-PI12-LF-10K <sup>†</sup>	

<sup>†</sup> To obtain Cisco Prime Infrastructure 1.4.1, order Cisco Prime Infrastructure 1.2 with a service contract and download Cisco Prime Infrastructure 1.4 and service pack 1 from Cisco.com. Existing customers with a valid service contract can also download Cisco Prime 1.4 and service pack 1. Customers without a valid service contract must purchase a service contract to gain access to the Prime Infrastructure 1.4 download on Cisco.com

# Appendix B: Changes

---

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

- We updated the Cisco Prime Infrastructure software to version 1.4.1.
- We rewrote the guide to align the use case, design overview, and deployment details with the Lifecycle view of the web-based GUI.

## 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](http://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.

© 2013 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](http://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)